

Règlement d'utilisation des technologies de l'information et des communications



SOMMAIRE

| | |
|--|----|
| Préambule..... | 4 |
| Section 1. Portée et opposabilité du règlement..... | 5 |
| 1.1. Définitions | 5 |
| 1.2. Objectifs du règlement..... | 5 |
| 1.3. Opposabilité du règlement..... | 6 |
| Section 2. Accès au système d'informations (SI) et gestion des documents et des données..... | 6 |
| 2.1 Sous-section - Accès au SI..... | 6 |
| 2.1.1. Fonctionnement et sécurité du SI..... | 6 |
| 2.1.2. Règles d'utilisation et d'usage sécurisé du SI..... | 6 |
| 2.2 Sous-section - Gestion des documents et des données..... | 8 |
| 2.2.1 Le plan de classement | 8 |
| 2.2.2 Le tableau de gestion (charte d'archivage)..... | 8 |
| Section 3. Utilisations du SI - cadre et limites..... | 9 |
| 3.1 Sous-section - Utilisations professionnelle et privée du SI..... | 9 |
| 3.1.1 Des règles et des responsabilités..... | 9 |
| 3.1.2 Le principe d'utilisation professionnelle/privée de la messagerie..... | 10 |
| 3.1.3 Messages personnels..... | 10 |
| 3.1.4 Réseaux sociaux..... | 10 |
| 3.1.5 Usage personnel du SI..... | 10 |
| 3.1.6 Accessibilité aux informations..... | 11 |
| 3.2 Sous-section - Autres utilisations du SI..... | 11 |
| 3.2.1. Utilisation des outils informatiques par les représentants du personnel..... | 11 |
| 3.2.2. Accès aux espaces communs de travail ou aux plates-formes collaboratives du SI..... | 11 |
| 3.2.3 Utilisations hors du SI départemental..... | 11 |
| Section 4. Utilisation des matériels et logiciels du Département..... | 12 |
| 4.1. Définitions..... | 12 |
| 4.2. Paramétrages de confort..... | 12 |
| 4.3. Changement d'affectation des matériels..... | 12 |
| 4.4 Périphériques..... | 12 |
| 4.5. Mobiles..... | 12 |
| 4.6. Antivirus et sécurité..... | 12 |
| 4.7. Postes extérieurs..... | 12 |
| 4.8. Perte, vol ou dégradation des matériels..... | 13 |
| Section 5. Vérifications et contrôles..... | 13 |
| 5.1. Filtrage et enregistrement des connexions sortantes..... | 13 |
| 5.2. Conservation des informations..... | 13 |
| 5.3 Finalités de la conservation des informations susvisées | 13 |
| 5.4 Utilisation non professionnelle..... | 14 |
| 5.5 Communication des informations en cas de contrôle..... | 14 |
| 5.6. Communication des informations en cas de réquisition judiciaire | 14 |
| Section 6. Confidentialité..... | 15 |
| 6.1. Utilisation du SI..... | 15 |
| 6.2. Choix et confidentialité du mot de passe..... | 15 |
| 6.3 Respect du droit de propriété intellectuelle..... | 15 |
| 6.4 Respect du droit de la vie privée..... | 15 |
| 6.5 Obligation de réserve..... | 15 |
| 6.6 Obligation de confidentialité..... | 15 |
| Section 7. Informatique, Libertés et protection des données à caractère personnel (DCP)..... | 16 |
| Section 8. Sanctions encourues en cas de non-respect du présent règlement..... | 16 |

| | |
|--|----|
| ANNEXE A _ Administrateurs et techniciens de la DOSIN et fonctionnement du SI départemental..... | 17 |
| A- 1. Sécurité et confidentialité..... | 17 |
| A- 2. Opérations de surveillance et de contrôle..... | 17 |
| A- 3. Opérations d'assistance et de maintenance..... | 18 |
| A- 4. Gestion des matériels..... | 19 |
| A- 5. Comptes administrateurs..... | 19 |
| A- 6. Traçabilité (journalisation)..... | 19 |
| A- 7. Sanctions..... | 19 |
| ANNEXE B _ Utilisation des smartphones personnels synchronisés avec la messagerie du Département..... | 20 |
| B- 1. Objet..... | 20 |
| B- 2. Prise en compte des risques d'utilisation..... | 20 |
| B- 3. Paramétrage..... | 20 |
| B- 4. Responsabilité..... | 20 |
| B- 5. Connexion..... | 20 |
| B- 6. Prise en charge..... | 20 |
| B- 7. Maintenance et Support..... | 21 |
| B- 8. Sécurité des données..... | 21 |
| ANNEXE C _ Délits pouvant être évoqués en cas de comportement de comportements illicites ou prohibés..... | 22 |
| C- 1. Consultation et/ou participation à des sites illicites pour laquelle le Département portera plainte contre l'agent qui fera également l'objet d'une procédure disciplinaire..... | 22 |
| C- 2. Consultation et/ou participation à des sites prohibés et pour lesquels un agent pourra faire l'objet d'une procédure disciplinaire..... | 22 |

Préambule

Le système d'informations recouvre l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, mis à la disposition des utilisateurs par le Département.

Le présent règlement définit les règles d'usages et de sécurité que le Département et chacun des utilisateurs s'engage à respecter.

Le cadre réglementaire actuellement en vigueur comprend le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) 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 et abrogeant la directive 95/46/CE, la loi Informatique et Libertés (LIL) modifiée et l'ordonnance 2018-115 du 12/12/2018 prise en application de l'article 32 de la LIL

Ce règlement pourra être modifié en particulier pour prendre en compte les évolutions des politiques de sécurité, de la réglementation et des progrès technologiques.

Entrée en vigueur

Il annule et remplace l'ensemble des dispositions précédentes.

Il a fait l'objet d'un avis en Comité Technique (CT) en date du et a été adopté par la

Commission Permanente en date du.....

Le règlement entrera en vigueur le ...

Bruno MAGGUILLI

Directeur Général Adjoint des Ressources

Section 1. Portée et opposabilité du règlement

Le présent règlement complète le cadre législatif. Il définit les droits et obligations des utilisateurs des ressources informatiques du Département de la Drôme. L'utilisateur est informé que sa propre responsabilité, celle de son service et la responsabilité du Département peuvent être engagées civilement et pénalement du fait de son comportement. Il veillera donc à respecter les lois et règlements en vigueur, ainsi que les règles d'utilisation, de sécurité et de bon usage décrites dans le présent règlement. Tout utilisateur du système d'informations de la collectivité n'ayant pas respecté ce règlement pourra faire l'objet de sanctions.

Le Département de la Drôme met à la disposition des personnels, un ensemble de ressources numériques (Internet, Intranet, messagerie, espaces collaboratifs, ordinateurs, imprimantes, photocopieurs, téléphones, etc.) logicielles et matérielles, **réservées aux activités professionnelles**. Les ordinateurs et les stations de travail sont connectés à un réseau local lui-même relié à Internet.

Il est interdit de consulter des sites dont le caractère est proscrit :

- sites contenant des données légalement interdits¹,
- sites interdits par le Département, dont l'usage est inapproprié avec les moyens mis à disposition : sites de contenus pornographiques, site dénigrant les institutions, sites de rencontre, sites réservés aux adultes, sites de jeux en lignes, sites de commerce en ligne. La liste n'est pas exhaustive.

L'annexe C détaille les délits pouvant être évoqués en cas de comportements illicites ou prohibés.

Toutefois, en cas de réception, sans les avoir demandés, de documents légalement interdits, l'agent en informe immédiatement sa hiérarchie et la DOSIN avant de les détruire. En effet, nos coordonnées électroniques pourraient être enregistrées par les administrateurs de ce genre de sites et exploitées ensuite dans des courriels comportant des pièces illicites.

La publication de données diffamatoires, sexistes, discriminatoires ou incitant à la violence sous toutes ses formes est assimilée à un délit. L'infraction est constituée dès la rédaction du message avant même sa diffusion. Il s'agit donc pour chacun d'être prudent dans l'usage des propos tenus à titre privé ou confidentiel.

1.1. Définitions

Le présent règlement avec ses annexes s'applique à l'ensemble des systèmes d'informations du Département de la Drôme et à tous leurs utilisateurs définis au point 1.3.

L'ensemble des systèmes d'informations intéresse notamment :

- L'informatique, soit entre autres : Internet, la messagerie électronique, la messagerie instantanée, les serveurs, logiciels et progiciels, les applications, bureautique et moyens d'impressions,
- Les matériels connectés au système d'informations et notamment : les ordinateurs, serveurs, périphériques, téléphones, imprimantes et scanners, ainsi que les matériels et logiciels mis à disposition dans le cadre du télétravail sont réservés à l'usage exclusif de l'agent, c'est-à-dire à l'exclusion de toute autre personne,
- Les équipements nomades, soit entre autres : les ordinateurs portables, tablettes, smartphones, clefs USB, disques durs externes, téléphones fixes et mobiles.

1.2. Objectifs du règlement

- Sécuriser l'utilisation du système d'information (SI) ;
- Encadrer les droits et responsabilités des utilisateurs ;
- Faciliter le travail quotidien des utilisateurs.

¹images ou textes pédophiles, à caractère raciste, concernant le trafic de stupéfiants ou pouvant porter atteinte aux fondamentaux de la Nation.

1.3. Opposabilité du règlement

Il est opposable à tout utilisateur du SI à compter de son entrée en vigueur. On entend indifféremment par « **utilisateur** » toute personne, employée ou non par le Département, amenée à utiliser l'un ou l'autre de ses systèmes d'informations de manière directe ou indirecte, permanente ou ponctuelle, y compris dans le cadre du télétravail. ; à savoir agent titulaire ou non titulaire de la fonction publique, élu, stagiaire, vacataire, apprenti, collaborateur occasionnel du service public, représentant des organisations syndicales, sous-traitant...).

Le règlement a un caractère obligatoire.

Chaque utilisateur est personnellement responsable du respect du présent règlement et de l'utilisation du SI de la collectivité. Le personnel encadrant est fondé à intervenir pour la mise en œuvre du présent règlement dans le cadre de son périmètre de responsabilité.

Section 2. Accès au système d'informations (SI) et gestion des documents et des données

2.1 Sous-section - Accès au SI

2.1.1. Fonctionnement et sécurité du SI

La DOSIN assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication du Département. Les agents habilités de cette direction disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Ils ont accès à l'ensemble des données techniques et sont tenus au respect des règles de confidentialité applicables aux contenus des documents et des supports des utilisateurs, ainsi qu'à la protection des données à caractère personnel. Ils sont assujettis dans l'exercice de leurs fonctions au devoir de réserve et sont tenus d'assurer et de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions (détail en annexe A).

La sécurité du SI mise en place par la DOSIN, vise la protection des informations et des données à caractère personnel, à travers leur disponibilité, c'est à dire accéder à chaque fois que de besoin aux informations et données utiles en fonction de son habilitation, leur intégrité, c'est à dire qu'elles ne soient pas dénaturées et leur confidentialité, c'est à dire veiller à ce qu'un tiers non autorisé n'ait pas accès à ces données.

2.1.2. Règles d'utilisation et d'usage sécurisé du SI

Chaque utilisateur doit être habilité pour se connecter au système d'informations.

2.1.2.1 Mot de passe

Chaque utilisateur est habilité par un mot de passe, individuel et inaccessible. Il est strictement confidentiel et ne doit ainsi pas être communiqué. L'identifiant délivré par la DOSIN (d26 intégrant le matricule de l'utilisateur) permet à celui-ci d'accéder au SI du Département.

- chaque utilisateur est responsable de l'utilisation qui peut en être faite,
- le mot de passe ne doit pas être communiqué ni noté sur des supports accessibles à autrui (ex. : l'inscrire sur un support papier à proximité du poste de travail),
- le mot de passe ne doit pas être facile à deviner (pas de prénom ou date de naissance de proches, par exemple),
- le mot de passe doit respecter, à tout moment, les règles de complexité mises en œuvre par la DOSIN, cf. politique du mot de passe, voir *lc@rré_boite à outils_ informatique-et-telephonie/connexion*
- le mot de passe est changé obligatoirement selon une périodicité liée au type de compte utilisé,
- si un collaborateur a un besoin de recherche sur votre poste de travail, il doit se connecter avec ses identifiant et mot de passe propres.

En cas d'oubli du mot de passe, une demande par mail à la boîte sos-info@ladrome.fr doit être faite par votre responsable hiérarchique. Cette mesure permet de lutter contre l'usurpation d'identité et d'assurer la traçabilité des modifications d'authentification. Ainsi, aucune modification de mot de passe ne peut être faite par téléphone.

Les connexions génériques (identifiant ou mot de passe partagés) sont interdites. Par dérogation accordée par le RSSI, et après validation interne de la Direction métier, la connexion générique peut être accordée dans un périmètre précis du SI.

2.1.2.2 Responsabilité de l'utilisateur

Tout utilisateur est responsable de l'utilisation qu'il fait du système d'informations, ainsi que du contenu de ce qu'il affiche, télécharge ou envoie. Il doit en permanence garder à l'esprit que c'est sous le nom du Département qu'il se présente sur Internet et doit respecter l'image de l'institution. Au même titre que pour le courrier, le téléphone ou la télécopie, chacun est responsable des messages envoyés et doit utiliser la messagerie dans le respect des missions et fonctions qui lui sont dévolues.

L'utilisateur ne doit pas accéder, tenter d'accéder, ou supprimer des informations si cela ne relève pas des tâches qui lui incombent.

2.1.3. Droits d'accès aux systèmes d'informations

Ils sont attribués et retirés au regard des fonctions ou missions de l'utilisateur, avec l'accord de sa hiérarchie. Ils cessent à la fin des fonctions exercées qui ont motivé leur attribution. Le supérieur hiérarchique direct de l'utilisateur informe la DOSIN concernant tout changement de missions affectant des droits.

2.1.3.1 Mesures de sécurité automatiques du SI départemental

En cas d'absence du poste de travail même momentanément, l'utilisateur doit le verrouiller. La mise en fonction automatique de l'économiseur d'écran avec verrouillage de la session, au bout de 15 minutes maximum d'inactivité, est mise en place de manière systématique pour des raisons de sécurité.

2.1.3.2 Départ de l'utilisateur de la collectivité

Lors du départ d'un utilisateur, pour assurer la continuité des services, l'utilisateur devra informer les usagers avec qui il est en relation de l'identité de son remplaçant et remettre à son chef de service ou son remplaçant les mails professionnels en sa possession. Son responsable doit s'assurer de la récupération des données professionnelles sur O:\, U:\ et dans la messagerie.

L'utilisateur doit supprimer l'ensemble des données personnelles qu'il aurait stocké sur le système d'informations du Département (lecteurs réseaux, poste de travail...).

La direction des ressources humaines saisit dans l'application RH la date de départ de l'utilisateur. Son compte utilisateur est alors désactivé pendant 1 mois puis supprimé à l'issue de ce délai.

Le Département prendra les mesures nécessaires pour obtenir la récupération des matériels auprès des agents qui omettraient de les rendre lors de leur départ.

2.1.3.3. Téléchargement et installation de logiciels

Toute installation de logiciel sur un poste informatique nécessite l'intervention de la DOSIN en local ou à distance, quand bien même le mot de passe administrateur ne serait pas requis. L'utilisation d'applications dites "portables" (sans installation) requiert impérativement un accord de la DOSIN. L'utilisateur doit s'assurer du respect des droits d'auteurs et de la propriété intellectuelle de ces applications.

2.1.3.4. Équipements étrangers à la collectivité

Avant toute connexion de matériels étrangers (disque dur externe, clé USB,) au Département sur un poste de travail, ceux-ci doivent obligatoirement avoir été contrôlés par un antivirus à jour au préalable. Ceci afin de limiter au maximum les risques de création d'une faille ou d'un incident de sécurité.

2.1.3.5 Suspension d'accès au SI totale, partielle ou temporaire

L'accès au SI départemental peut-être suspendu à titre de mesure conservatoire, sur demande du responsable de la sécurité du système d'informations (RSSI), pour des raisons de sécurité de façon totale, partielle ou temporaire.

La suspension des droits de l'/des utilisateur/s à ce titre n'est pas utilisable comme une sanction de l'utilisateur.

2.1.3.6 Continuité de service

En cas d'absence d'un agent, l'accès notamment à son poste informatique, à sa messagerie électronique et à ses données **non privées** peut être justifié par la continuité du service, s'il n'est pas possible d'attendre son retour. Cet accès ne peut en aucun cas se traduire par une communication du mot de passe de la messagerie individuelle à un/e collègue. La DOSIN est alors sollicitée par le directeur hiérarchique de l'agent pour accéder aux informations nécessaires à la continuité du service.

Dans tous les cas, l'utilisateur doit être informé par sa hiérarchie et par écrit, des mesures affectant ses droits ou des opérations effectuées en son absence sur ses données et son poste de travail dans le respect du point 3.1.5.

2.2 Sous-section - Gestion des documents et des données

Les utilisateurs sont amenés à ouvrir des répertoires sur le réseau O:\ (ou un autre serveur) et reprendre des fichiers dans des répertoires existants, ou à utiliser des applications informatiques, tout cela en parallèle des dossiers sur support papier.

Il s'agit dans tous les cas d'archives publiques qui doivent être gérées selon des dispositions légales.

Chaque agent est responsable des **archives électroniques et papier** qu'il produit.

Les dossiers d'activité sont aujourd'hui le plus souvent hybrides, ils sont constitués très souvent à la fois de documents sur support papier et d'autres sur support électronique.

Au quotidien, bien gérer les fichiers bureautiques et les courriels, en parallèle des dossiers papier, limite les risques dans la gestion des documents et de leurs données et respecte le RGPD. Sont à mettre en œuvre :

2.2.1 Le plan de classement

Son objectif : faciliter la gestion des documents bureautiques et permettre un archivage futur.

Il définit l'emplacement et les droits d'accès des documents papiers ou électroniques. Il est obligatoire pour tous les services et s'applique à tous les agents dès validation hiérarchique par une note de service. Les mails doivent être soit édités en pdf et intégrés au plan de classement dans le dossier correspondant, soit détruits s'ils ne présentent pas d'intérêt administratif, juridique ou historique.

2.2.2 Le tableau de gestion (charte d'archivage)

Il définit la durée de vie des données qu'elles soient sur support papier ou électronique et leur sort final (versement, destruction, tri...). Il est co-élaboré et co-validé par le service producteur et les Archives départementales. Il est obligatoire et s'applique à tous dès validation. Il est à disposition des agents sur *Ic@rré_Boîte à outils → Archivage → Chartes d'archivage et tableaux de gestion*

Le plan de classement et le tableau de gestion **sont les prérequis à l'archivage réglementaire des données**. Les outils juridiques obligatoires pour répondre au code du patrimoine sont les bordereaux de versement et d'élimination. Un correspondant « Archives » a été identifié dans chaque direction et/ou service.

L'archivage papier et électronique sont indissociables. Il est impossible de gérer séparément les fichiers bureautiques, les courriels, les données issues des applications informatiques et les dossiers papier : à chaque fois qu'une élimination ou un versement est envisagé, il faut se poser la question pour le support papier et pour le support électronique. Le tableau de gestion est l'outil qui permet de gérer ces deux supports à la fois.

Section 3. Utilisations du SI - cadre et limites

3.1 Sous-section - Utilisations professionnelle et privée du SI

Les systèmes d'informations (messagerie, internet...) sont des outils de travail réservés à titre principal à des usages professionnels. En effet, selon l'article 25 septies, alinéa 1er de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, "le fonctionnaire consacre l'intégralité de son activité professionnelle aux tâches qui lui sont confiées". La messagerie doit être utilisée en ayant conscience des usages interdits qui sont décrits dans l'annexe C.

Sauf s'ils sont expressément identifiés comme privés, toute donnée et tout échange sont réputés professionnels.

3.1.1 Des règles et des responsabilités

3.1.1.1. Adresses électroniques

Le Département met à disposition une boîte à lettres professionnelle nominative nous permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse nominative s'effectue ensuite sous la responsabilité de l'utilisateur.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.

En ce sens, une adresse électronique @ladrome.fr engage la collectivité et donc doit être conforme à son image et à ses principes (respect des principes républicains, respect des règles de politesse, etc...)

Une adresse électronique fonctionnelle ou organisationnelle peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins du Département.

3.1.1.2. Confidentialité

Les données circulant sur la messagerie électronique internet ne sont pas protégées, notamment contre les détournements éventuels (destruction des informations, perte ou modification intentionnelle). Les messages comportant des données confidentielles ne doivent pas être diffusés par la messagerie internet. En revanche, l'envoi à une adresse interne permet de faire circuler de telles données car ce circuit est protégé. Lorsque les données sont sensibles, une sécurisation de l'envoi est requise. L'utilisateur trouvera sur l'intranet les procédures adaptées pour effectuer cet envoi.

Il est rappelé à l'utilisateur que sa responsabilité est protégée par la sécurité de son mot de passe. L'usurpation d'identité ou la tentative d'usurpation d'identité, en vue d'accéder aux ressources informatiques, est passible de sanctions.

3.1.1.3 Emission et réception des messages

Chaque utilisateur s'assure de l'identité et de l'exactitude des adresses des destinataires des messages.

Chaque utilisateur veille à ce que la diffusion des messages soit limitée aux seuls destinataires concernés (respect de la confidentialité). Ce qui évite aussi les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

En conséquence, il faut être vigilant sur la nature des messages électroniques échangés, au même titre que pour les courriers traditionnels.

3.1.1.4 Courriel vaut écrit

Les règles habituelles en matière de communication écrite s'appliquent pleinement à la messagerie électronique. Les procédures applicables à tout courrier ou toute transmission d'information doivent donc être respectées : le contrôle, la validation ou l'information du responsable hiérarchique, le niveau de signature de son auteur.

Un message électronique peut être une preuve ou un commencement de preuve, et chacun est responsable des informations qu'il est autorisé à diffuser ou à publier sur le réseau interne de la collectivité. Les risques encourus sont aussi grands avec un message électronique qu'avec un document papier. Il existe un risque réel d'insérer dans un message électronique des engagements sur lesquels il pourra être difficile de revenir. Le devoir de réserve s'applique pour tout message électronique adressé à partir de la messagerie du Département.

3.1.1.5 Utilisation des boîtes fonctionnelles

Une adresse électronique fonctionnelle, boîte aux lettres générique, à usage strictement professionnel, peut être mise en place, pour un utilisateur ou un groupe d'utilisateurs pour les besoins du Département. Le gestionnaire et les personnes habilitées à accéder à cette boîte sont responsables de son utilisation. Pour des raisons de continuité de service, l'adresse générique est liée à la mission et non à un utilisateur.

3.1.2 Le principe d'utilisation professionnelle/privée de la messagerie.

Il existe un principe de respect de la vie privée sur le lieu de travail. Ce principe, issu à la fois de la loi et de la jurisprudence, prévoit que tout salarié ou agent a droit au respect de sa vie privée sur son lieu de travail. Dans ce cadre, toute donnée, fichier et/ou document issus de la correspondance électronique (courriel) spécifiquement identifié comme personnel, dossier nommé personnel ou privé n'est pas accessible à l'employeur, sauf selon les exceptions indiquées ci-dessous du point 3.1.5.

À contrario, tout autre fichier de même nature dont n'est pas spécifié le caractère personnel est présumé relever de la sphère professionnelle et, par voie de conséquence, accessible à l'employeur.

3.1.3 Messages personnels

L'usage de la messagerie électronique est réservé à un usage professionnel, sauf exception qui doit être rare et se faire alors en dehors des heures de travail. Les messages personnels ne doivent pas contrevenir aux lois, ni aux règles édictées pour les messages professionnels (réserve, confidentialité...) : dans ce cas, les correspondances échangées ne bénéficient pas de la protection liée à la correspondance privée. Ils doivent par ailleurs rester marginaux.

3.1.4 Réseaux sociaux

À l'exception de la consultation des informations publiées par le Département ou de ses partenaires dans le cadre professionnel, toute participation aux réseaux sociaux (Facebook, Twitter...) est considérée comme un usage privé, tolérée sous réserve du respect des conditions décrites dans cette section.

3.1.5 Usage personnel du SI

A titre subsidiaire, il est toléré que les outils du SI soient utilisés pour des usages privés pendant les temps de pause. Ces utilisations se font dans le respect des dispositions légales et réglementaires, à la condition expresse de respecter les dispositions du présent règlement. Cet usage ne doit en aucun cas porter atteinte au bon fonctionnement du service, être préjudiciable à la bonne réalisation de l'ensemble de ses missions par l'utilisateur (cf. article 5.4 du présent règlement) ou porter atteinte à l'image de la collectivité.

Cet usage ne peut être contraire à l'ordre public et aux bonnes mœurs ni contrevenir aux lois et règlements en vigueur ou aux règles déontologiques, éthiques ou morales opposables aux agents publics. A ce titre, toute utilisation abusive peut donner lieu à sanction.

L'identification d'un répertoire, d'un fichier ou d'un courriel privé doit être clairement identifiée et rangée dans des dossiers distincts du plan de classement par leur nomination en objet (message électronique) des termes « PRIVÉ », « PERSONNEL » ou « PERSO », suivi du nom et prénom de l'utilisateur. Il est possible, dans le respect de la législation en vigueur, de procéder au stockage de vos données à caractère privé sur notre poste de travail exclusivement (lecteur G).

Les ressources réseau (lecteurs O:\ V:\) sont réservées à un usage professionnel. La DOSIN est responsable des espaces de stockage des données à caractère privé **et lors du départ définitif de l'agent du service, elle supprime les données personnelles si l'agent ne l'a pas fait lui-même.**

3.1.6 Accessibilité aux informations

À des fins de continuité de service, la DOSIN prend les mesures nécessaires afin de permettre l'accès aux ressources professionnelles mises à notre disposition (dossiers partagés...).

L'accès à des données privées par un tiers, est strictement interdit en raison de la protection de la vie privée et/ou du secret des correspondances.

Utilisation partagée et individuelle du système d'informations

- partagée : les espaces informatiques c'est-à-dire accessibles et utilisés par plusieurs utilisateurs en fonction des droits qui leur sont attribués (espaces « O : » , « V : », espaces collaboratifs),
- individuelle : c'est-à-dire accessibles et utilisés par un seul utilisateur (espace « G : », messagerie professionnelle) ou toute autre nomenclature pouvant s'y substituer.

Poste partagé par plusieurs personnes

Chaque utilisateur ouvre sa propre session à l'aide de son mot de passe et ferme la session en cours lorsqu'il quitte le poste de travail partagé (même pour une courte durée).

3.2 Sous-section - Autres utilisations du SI

3.2.1. Utilisation des outils informatiques par les représentants du personnel

Les représentants du personnel utilisent, dans le cadre de leur mandat, les outils informatiques qui leur sont attribués pour l'exercice de leur activité professionnelle. Ils disposent d'une adresse électronique ainsi que d'un espace Intranet dédié.

Les messageries syndicales

Les courriels adressés exclusivement aux syndicats sont réputés privés. Les messageries syndicales sont protégées par le secret des correspondances privées. Les messageries nominatives individuelles des représentants syndicaux sont soumises aux mêmes règles que celles des autres agents.

3.2.2. Accès aux espaces communs de travail ou aux plates-formes collaboratives du SI

L'information est classée et restreinte à ceux qui en ont l'usage. Par conséquent, les personnels encadrant sont légitimes et ont le devoir :

- d'organiser et promouvoir des plans de classement au sein des espaces sous leur sphère de responsabilité ;
- de définir les accès en lecture ou en écriture et dans leur périmètre sur une partie des plans de classement lorsque la confidentialité l'exige, notamment pour les données à caractère personnel incluant les données sensibles.

3.2.3 Utilisations hors du SI départemental

L'utilisateur doit être conscient que les règles d'éthique professionnelle, de déontologie, de secret et de réserve professionnels qui s'appliquent aux logiciels internes, s'étendent également aux

communications réalisées en dehors des systèmes d'information du Département, et notamment sur les forums, réseaux professionnels et réseaux sociaux.

Toutes les dérives perpétrées dans ce cadre, et notamment injure, diffamation, atteinte à la vie privée ou manquement au devoir de réserve sont de nature à justifier des sanctions disciplinaires, voire des poursuites civiles et/ou pénales de l'utilisateur.

Section 4 Utilisation des matériels et logiciels du Département

4.1. Définitions

Sauf indication contraire, sont entendus par « matériels » tout équipement support ou vecteur des systèmes d'informations définis au lexique.

4.2. Paramétrages de confort

Ils sont réalisés par les utilisateurs afin de personnaliser les matériels mis à leur disposition.

Sont autorisés : l'ergonomie du poste, le positionnement de matériels dans un même bureau, le son, la luminosité, l'affichage, etc.

4.3. Changement d'affectation des matériels

D'une manière générale, un équipement permettant l'utilisation du système d'informations du Département (ordinateur, téléphone, périphérique...) est attribué à un poste budgétaire et non à un agent :

- l'agent change de bureau : le matériel déjà attribué reste affecté à son poste,
- l'agent change de poste : le matériel sera celui de sa nouvelle affectation.

Le déplacement hors d'un même bureau, la permutation ou la destruction de matériels sont effectués exclusivement par la DOSIN ou sous son contrôle.

En cas de suppression du poste, l'équipement est récupéré par la DOSIN.

4.4 Périphériques

L'utilisation de périphériques de stockage privés compatibles USB est tolérée sans autorisation préalable, sous réserve que l'utilisateur ne dépose pas d'informations de nature à nuire à la sécurité informatique. Tout autre périphérique privé devra être autorisé et installé par la DOSIN.

Les périphériques professionnels autorisés sont fournis et/ou installés par la DOSIN.

4.5. Mobiles

Les téléphones mobiles sont livrés avec une carte SIM et un chargeur. Certains téléphones mobiles qui sont connectables sur le poste de travail, ne le seront qu'avec les câbles fournis avec l'appareil. Si un logiciel est nécessaire, il est obligatoirement installé avec l'accord et l'intervention de la DOSIN. L'utilisateur devra assumer les coûts éventuels des applications personnelles installées sur les smartphones.

4.6. Antivirus et sécurité

Il est formellement interdit de désactiver les logiciels de sécurité comme par exemple les pare-feux et les antivirus. Si la configuration de ces derniers paraît entraver une action légitime, la DOSIN doit être sollicitée. Les utilisateurs doivent être particulièrement vigilants lorsqu'ils se connectent sur des réseaux autres que celui du Département de la Drôme, puisqu'ils perdent alors le bénéfice des équipements de sécurité et de sauvegarde placés sur le réseau.

4.7. Postes extérieurs

La connexion de postes informatiques n'appartenant pas au Département de la Drôme, c'est-à-dire non configurés et paramétrés par nos services est interdite, sauf :

- dans le cadre d'une connexion WIFI temporaire. Les demandes sont conservées pendant 1 an,

- si une application ou une ressource interne du Département de la Drôme est configurée et adaptée pour être accessible depuis Internet (extranets, messagerie professionnelle, site institutionnel, etc.). Les utilisateurs peuvent y accéder depuis n'importe quel navigateur à l'aide d'un compte valide.

4.8. Perte, vol ou dégradation des matériels

L'utilisateur est tenu d'informer la Dsin dans les meilleurs délais.

Dans le cas où le matériel contenait des données à caractère personnel, il est tenu d'en informer dans les meilleurs délais, la déléguée à la protection des données du Département (dpd@ladrome.fr).

Section 5. Vérifications et contrôles

Ils concernent **tous** les utilisateurs du SI.

5.1. Filtrage et enregistrement des connexions sortantes

Toutes les URL de navigations (sites web) sont connues et conservées pendant un an maximum, y compris celles qui sont réalisées à partir d'un protocole sécurisé HTTPS.

5.2. Conservation des informations

Sont conservées de manière automatique durant une période de 1 an les informations suivantes :

- l'adresse appelée URL (par exemple www.ladrome.fr),
- l'heure de connexion,
- l'adresse IP du poste et des serveurs sollicités (exemple 157.157.123.456),
- toutes les traces de courrier électronique réceptionné et émis par le serveur de messagerie (logs),
- le numéro appelé, l'heure, la durée et le coût de tous les appels téléphoniques externes passés par les postes téléphoniques fixes ou mobiles. Les quatre derniers chiffres sont obligatoirement masqués sur le suivi de consommation,
- le volume des impressions en nombre de pages,
- la place occupée sur le système d'informations.

La durée de conservation de la facturation est de 10 ans conformément à la réglementation en vigueur.

5.3 Finalités de la conservation des informations susvisées

Conformément au respect de la vie privée des personnes concernées (utilisateurs du SI), les informations susvisées sont conservées pendant 1 an à partir de leur collecte et ce pour les objectifs suivants :

- la récupération des informations de connexion en cas de malveillance caractérisée ou non-respect de la règle en vigueur,
- la gestion de l'annuaire téléphonique interne (constitution, édition et diffusion de listes nominatives des utilisateurs des services téléphoniques),
- la gestion technique de la messagerie interne,
- le remboursement des services de téléphonie utilisés à titre privé par les employés lorsque le caractère privé de l'utilisation de ces services est déterminé par les employés eux-mêmes comme indiqué au point 4.5.,
- la maîtrise des dépenses liées à l'utilisation professionnelle des services de téléphonie (établissement et édition des relevés liés à l'utilisation des services de téléphonie, calcul du coût de cette utilisation et établissement de statistiques anonymes),
- la maîtrise des dépenses liées à l'utilisation effectuée à titre privé des services de téléphonie.

Sont notamment exclus :

- l'écoute ou l'enregistrement des communications sauf cas particulier et justifié avec accord de l'agent concerné,
- la surveillance de l'activité d'un employé à partir de l'usage de son téléphone mobile,
- l'édition de statistiques et la consultation des journalisations des correspondances des lignes des organisations syndicales.

5.4 Utilisation non professionnelle

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

5.5 Communication des informations en cas de contrôle

Pour les données téléphoniques

En cas de consommation manifestement anormale des services utilisés, le relevé des justificatifs des numéros de téléphones appelés pourra être établi avec les 6 premiers chiffres des numéros.

En cas d'abus manifeste ou de comportement inapproprié de la part de l'agent

Cet abus est relatif aux informations collectées indiquées précédemment au point 5.2. Avant toute prononciation d'éventuelles sanctions, des mesures conservatoires peuvent être placées en urgence afin de restreindre les droits et accès d'un utilisateur si ce dernier peut faire courir un risque à la collectivité, aux usagers ou à ses collègues.

Après information de l'agent, après avis de la direction des ressources humaines, après validation du directeur et de la direction générale, les personnels encadrants ont la possibilité, sauf exceptions éventuelles prévues au protocole syndical et au point 5.3, d'accéder ou de vérifier via la DOSIN, l'ensemble des informations suivantes :

- les fichiers et courriels d'un agent non identifiés comme privés (cf. 4.1.4) ;
- les relevés détaillés des consommations téléphoniques,
- les connexions Internet (informations de connexion : URL uniquement, pas le contenu).

Ces demandes spécifiques et ponctuelles sont consignées par la direction des ressources humaines. Ce recueil est porté à la connaissance de la DPD du Département. Les limites de l'action des techniciens informatiques sont indiquées en annexe A.

5.6. Communication des informations en cas de réquisition judiciaire

Dans ce cas, les numéros de téléphones appelés pourront être établis avec les 10 chiffres. De même les fichiers et échanges identifiés comme privés ou masqués pourront être transmis en clair aux autorités compétentes, uniques destinataires de ces données et sur présentation d'une commission rogatoire ad hoc.

Section 6. Confidentialité

6.1. Utilisation du SI

Elle est loyale et respectueuse d'autrui et de la collectivité. Elle vise à respecter le présent règlement et en particulier :

- à ne pas masquer son identité ni usurper celle d'un autre,
- à respecter le cadre d'usage des systèmes d'informations mis à sa disposition,
- à respecter les consignes de sécurité diffusées par la DOSIN et par sa hiérarchie,
- à ne jamais communiquer ses mots de passe et à les changer sans délai si la consigne n'a pas pu être respectée,
- à ne pas divulguer, sans besoin reconnu, les coordonnées d'autres utilisateurs, et, si tel était le cas, à en informer les intéressés,
- à signaler à la DOSIN, qui en réfère au RSSI, toute violation ou tentative de violation de ses droits ou de façon générale toute anomalie constatée. Le RSSI informe la DPD si des données personnelles sont présentes.

6.2. Choix et confidentialité du mot de passe

Chaque utilisateur est personnellement responsable du choix de son/ses mot/s de passe.

Pour l'établir, il pourra se référer à cette fin au document correspondant, en vue d'en assurer une robustesse suffisante et disponible sur l'ic@rré, *Boîte à outils_Informatique et téléphonie* → *Connexion* → *Changement-MDP*.

6.3 Respect du droit de propriété intellectuelle

Tout utilisateur ne doit pas reproduire, copier, télécharger, diffuser, modifier ni utiliser les logiciels, bases de données, pages web, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

6.4 Respect du droit de la vie privée

Le droit à la vie privée, le droit à l'image et le droit de représentation impliquent qu'aucune image ou information relative à la vie privée d'autrui ne doit être vue sans l'autorisation de la personne intéressée.

6.5 Obligation de réserve

Tout agent public doit faire preuve de réserve et de mesure dans l'expression écrite et orale de ses opinions personnelles. Cette obligation impose aux agents publics d'éviter en toutes circonstances les comportements susceptibles de porter atteinte à la considération du service public par les usagers. Cette obligation de réserve ne concerne pas le contenu des opinions mais leur mode d'expression, celle-ci s'applique pendant et hors du temps de service.

6.6 Obligation de confidentialité

Tout utilisateur est tenu de respecter la confidentialité des informations auxquelles il a accès ou qu'il gère, conformément aux obligations de secret professionnel et de discrétion. Cette obligation s'applique tant pour le traitement des informations que pour leur communication interne et externe.

Section 7. Informatique, Libertés et protection des données à caractère personnel (DCP)

Parmi les données, certaines sont nominatives ou à caractère personnel. Elles sont alors soumises au RGDP et à la Loi Informatique et Libertés modifiée. Les utilisateurs amenés à collecter et gérer ces DCP, quel que soit leur fonction au sein de la collectivité départementale, s'engagent :

- à associer la/le DPD, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel,
- à informer la/le DPD de toute création ou modification d'un traitement dans le but de mettre à jour les inscriptions des traitements au registre de la collectivité, que la collectivité soit responsable de traitement ou sous-traitant de données à caractère personnel,
- à informer la/le DPD après la suppression d'un traitement devenu obsolète dans le but de mettre à jour le registre de la collectivité,
- à donner accès à la /au DPD, aux données à caractère personnel et aux opérations de traitement,
- à n'utiliser ces données que pour les strictes finalités pour lesquelles elles sont déclarées que la collectivité soit responsable de traitement ou sous-traitant,
- à ne diffuser les informations correspondantes qu'aux destinataires visés au registre pour les traitements considérés,
- à archiver les données dans les délais légaux afin de respecter le « droit à l'oubli »,
- à respecter les règles en matière de sécurité et de confidentialité fixées pour le traitement inscrit au registre et au présent règlement,
- à respecter le secret professionnel attaché à la connaissance de ces informations,
- à répondre, en moins d'un mois, aux demandes des usagers qui font valoir leurs droits sur leurs données en prenant appui auprès de la DPD si nécessaire,
- à signaler auprès de la DPD en moins de 48h toute perte ou vol de support contenant des données personnelles.

La/le délégué/e désigné/e par la collectivité a une mission d'accompagnement et de conseil auprès des utilisateurs et des services, et ne reçoit aucune instruction en ce qui concerne l'exercice des missions_ voir sur lc@rrr_Boite-a-outils→ [informatique-liberte-et-protection-des-donnees](#)→ [quelles-sont-les-personnes-ressources-de-la-protection-des-donnees](#)→ [dpd-ou-dpo-delegue-a-la-protection-des-donnees](#).

Section 8. Sanctions encourues en cas de non-respect du présent règlement

Tout utilisateur ne respectant pas les règles et obligations définies dans ce règlement est passible de sanctions disciplinaires ou contractuelles et s'expose selon la gravité des infractions à des poursuites pénales ou civiles conformément aux dispositions légales en vigueur.

Le dialogue sera alors privilégié, le cas échéant.

ANNEXE A _ Administrateurs et techniciens de la DOSIN et fonctionnement du SI départemental

Sous ce vocable, sont regroupés l'ensemble des agents de la DOSIN (administrateurs et techniciens) en charge de la gestion, de l'exploitation, de l'administration du parc matériel et logiciels, des bases de données et de la sécurité des systèmes d'informations du Département afin d'en assurer le bon fonctionnement.

Préambule - Déontologie des administrateurs réseaux et techniciens de la DOSIN

Les administrateurs et les techniciens dûment habilités par le directeur de la DOSIN, sont soumis au devoir de réserve et au secret professionnel.

Dans le cours normal de l'administration des systèmes, les administrateurs peuvent avoir à examiner des données afin d'obtenir suffisamment d'informations pour diagnostiquer et corriger des problèmes avec les logiciels, ou pour déterminer si un utilisateur agit en violation des règles énoncées plus haut. Les administrateurs ont le droit de procéder ainsi, mais ils ont l'obligation de préserver la confidentialité des informations privées des utilisateurs qu'ils ont été amenés à connaître dans ce cadre, sauf si celles-ci sont pénalement condamnables.

Ils ont obligation de n'accéder qu'aux données informatiques nécessaires à l'accomplissement de leurs missions et d'en assurer la confidentialité. Ils ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de la collectivité. Ils ne sauraient non plus être contraints de le faire.

Les administrateurs et les techniciens des systèmes d'informations respectent l'intégralité du présent règlement comme tous les utilisateurs des systèmes d'informations du Département, sous réserve des dispositions de la présente annexe.

Cette dernière a en particulier pour objet :

- de garantir le respect du secret des correspondances privées prévu par l'article L.432-9 du Code pénal,
- de garantir la sécurité des traitements dont ils assurent le support et l'exploitation prévue par les articles 24, 25 et 32 du RGDP et l'article 57 de l'ordonnance n° 2018-1125 du 12/12/2018 relative à l'Informatique et aux Libertés,
- de garantir le secret des communications électroniques.

A- 1. Sécurité et confidentialité

La sécurité des systèmes d'informations est assurée par la DOSIN. Pour garantir la sécurité et les échanges de données à caractère personnel, les techniciens à la demande des services fournissent les outils nécessaires pour assurer ces garanties.

Toute exploitation des informations dont les administrateurs et les techniciens ont connaissance, à des fins autres que celles liées à leurs missions est interdite y compris sur l'ordre de leur supérieur hiérarchique sauf en cas de risques d'altération, de dysfonctionnement des systèmes d'informations ou en cas de contrôle (cf. 5.5 du règlement).

A- 2. Opérations de surveillance et de contrôle

2.1. Contrôle visé au point 5.5 du règlement

Afin de garantir la continuité de service et la sécurité du système d'informations, les administrateurs et les techniciens **habilités** surveillent un ensemble de statistiques comme les flux réseaux, les connexions, les espaces disques des serveurs, les disques des postes utilisateurs, les imprimantes ou les consommations des équipements téléphoniques.

Si lors de ces surveillances ou audits des anomalies sont détectées, comme par exemple, sans que ce soit exhaustif :

- la présence de logiciels malveillants,

- la présence de programmes ou logiciels n'appartenant pas au parc logiciel de la collectivité,
- un taux anormalement élevé d'occupation des emplacements disques, commun ou individuel,
- une consommation trop importante de la bande passante en regard des missions des services,
- des appels vers des destinations inhabituelles ou coûteuses ;

les administrateurs et les techniciens ont obligation de le signaler auprès de leur hiérarchie.

Cette dernière en vérifiera le bien fondé en informant le ou les services concernés.

Dans le cadre de ces missions de contrôle, les personnels informatiques **ont interdiction formelle d'ouvrir ou d'accéder aux données des agents ou des services**, c'est-à-dire de lire à l'intérieur des fichiers ou de prendre connaissance du contenu d'un courriel ou d'une communication téléphonique (cf. section 3 du règlement). L'agent est astreint à garder le secret absolu sur ce contrôle **y compris envers ses collègues**. Cette exploitation globale est la même pour tous les utilisateurs du système d'informations.

2.2. Contrôle visé au point 5.6 du règlement

Ce type de contrôle **est déclenché par une réquisition judiciaire**. Le déroulement est le même que pour le contrôle du point 5.5, sauf qu'il n'y a pas de notion de données protégées par la vie privée si la réquisition est rédigée en ce sens.

A- 3. Opérations d'assistance et de maintenance

3.1. Opérations de maintenance des serveurs et ressources communes

Dans le cadre des opérations de maintenance ou d'exploitation les données peuvent être techniquement déplacées, dupliquées et sauvegardées qu'elles soient sur des disques, dans une application ou incluses dans la messagerie.

Dans le cadre de ces opérations courantes les personnels informatiques n'accèdent pas au détail des données et des fichiers.

Si pour des raisons techniques ou par mégarde un tel accès se produisait, le technicien est astreint au plus strict secret professionnel et doit limiter son accès au strict minimum nécessaire pour terminer son travail.

3.2. Opérations de maintenance sur les postes utilisateurs ou sur des terminaux mobiles

Lors des réparations ou remplacements des postes il est permis de demander le mot de passe d'accès aux ressources de l'utilisateur. Cet accès ne peut être utilisé que dans le cadre temporaire de la migration du poste et pour permettre de migrer les données locales.

Le mot de passe peut aussi être demandé lors de la configuration du compte de messagerie d'un terminal mobile.

L'utilisateur devra changer son mot de passe une fois l'opération terminée. Cette recommandation doit lui être systématiquement rappelée et sa mise en œuvre expliquée s'il le demande.

3.3. Prises de contrôle à distance des postes

Dans le cas particulier des prises de main à distance sur les postes, la prise de contrôle ne peut se faire que sur accord de l'utilisateur, c'est à dire après une action volontaire de sa part.

Toute prise de main à distance non autorisée par l'utilisateur par ce moyen est rigoureusement interdite et doit être stoppée immédiatement si elle est fortuite.

Il n'est pas autorisé dans un contexte d'exploitation normal de « dévalider » les paramètres qui concernent l'accord de l'utilisateur lors des prises de mains à distance. Seuls des contrôles visés aux points 5.5 et 5.6. du règlement, peuvent conduire à déroger à cette règle, ces contrôles ne peuvent être réalisés qu'après une demande écrite transmise par voie hiérarchique et en aucun cas par la seule initiative d'un technicien.

Les serveurs ou équipements qui ne sont pas affectés nominativement à un agent ou un groupe d'agents sont exclus de cette mesure puisqu'ils n'ont par nature pas d'utilisateurs. Ces

équipements peuvent seuls faire l'objet d'une prise de main à distance sans l'accord d'un utilisateur.

A- 4. Gestion des matériels

4.1. Stockage

Les matériels inutilisés contenant potentiellement des données doivent être stockés dans des locaux fermés à clé en attendant leur réutilisation ou destruction.

Les bandes de sauvegardes ne peuvent être conservées que dans la salle serveurs dans le cadre des opérations de sauvegarde ou dans un coffre.

4.2. Destruction

Les matériels pouvant contenir des données doivent être rendues illisibles. Le choix des moyens employés, logiciels ou physiques, est laissé à l'appréciation du service qui procède à l'opération.

A- 5. Comptes administrateurs

Les comptes administrateurs ne doivent être utilisés que lorsqu'il n'est pas possible de réaliser l'opération avec son propre compte. L'ensemble des opérations d'administration réalisés sur le système d'informations est enregistré.

A- 6. Traçabilité (journalisation)

Les serveurs enregistrent systématiquement les opérations effectuées et le compte utilisé. Les traces des serveurs sont conservées pendant **un an au maximum** à compter de leur enregistrement.

Il est formellement interdit de dévalider ou contourner le système de traces qui entoure les opérations d'exploitation normale, de se rendre anonyme ou d'usurper l'identité d'un autre administrateur ou utilisateur.

A- 7. Sanctions

Le non-respect des dispositions de la présente annexe expose aux mêmes sanctions que celles fixées par le présent règlement.

ANNEXE B _ Utilisation des smartphones personnels synchronisés avec la messagerie du Département

B- 1. Objet

La présente annexe définit les règles à respecter dans le cadre de la synchronisation des smartphones **personnels** pour accéder à la messagerie et à l'agenda professionnels.

On appelle « matériel » un équipement de type Smartphone ou Tablette.

Seuls les matériels fonctionnant sous IOS (Apple), Android (Samsung, Google, ...) ou validés par la DOSIN seront autorisés. La mise à disposition de la procédure de connexion ne sera pas communiquée pour les matériels non précisés ci-avant.

Cette annexe concerne toute personne désirant utiliser son matériel personnel dans le cadre professionnel cité ci-avant.

B-2. Prise en compte des risques d'utilisation

L'utilisation de matériels mobiles personnels (ex : iPhone, Android) engendre des risques que la DOSIN et l'utilisateur concernés se doivent de prendre en compte. Afin de minimiser les risques inhérents à ce type d'accès, l'utilisateur devra prendre en compte les bonnes pratiques suivantes :

- installer, sous réserve qu'il soit disponible, sur son matériel un logiciel antivirus,
- systématiser l'activation par mot de passe (protection par code PIN fiable) et d'autres procédés limitant l'accès au matériel,
- verrouiller automatiquement par mot de passe l'écran du matériel en cas de d'inactivité de celui-ci, pour empêcher la consultation en cas de perte ou de vol,
- procéder à la mise à jour du système d'exploitation dès qu'une nouvelle version est disponible,
- vérifier les conditions d'utilisation lors de l'installation d'applications,
- dans les lieux publics, privilégier les points d'accès sécurisés (par un mot de passe) aux points d'accès libres,
- relever le numéro IMEI de l'appareil afin de bloquer celui-ci en cas de perte ou de vol,
- ne pas stocker de données professionnelles sur son matériel personnel.

B- 3. Paramétrage

Le paramétrage du matériel personnel de l'utilisateur pour l'accès à sa messagerie et son agenda professionnels sera effectué par l'utilisateur lui-même à sa propre initiative. Il sera référencé à la DOSIN comme utilisateur de la messagerie et de l'agenda à partir de son matériel personnel.

La DOSIN fournira à l'utilisateur une procédure adaptée à son matériel. En aucun cas, ce paramétrage ne peut être imposé par son supérieur hiérarchique. L'utilisateur s'engage à ne pas communiquer ce paramétrage à un tiers, qu'il soit extérieur à la collectivité ou qu'il soit un utilisateur de la collectivité.

B- 4. Responsabilité

L'utilisateur a connaissance que ce paramétrage peut engendrer (rarement) des soucis de fonctionnement d'une autre application.

La DOSIN décline toute responsabilité liée à un dysfonctionnement du matériel.

B- 5. Connexion

La synchronisation avec la messagerie et son agenda électronique se fera via la connexion de l'appareil, connexion contractée avec son opérateur personnel. Le matériel ne sera **pas** connecté au réseau WIFI du Département.

B- 6. Prise en charge

Le Département ne prendra pas à sa charge, que ce soit en totalité ou partiellement, le coût de l'abonnement DATA du matériel de l'utilisateur, ni la mise à jour des licences ou applications.

Les éventuels surcoûts liés à des dépassements de forfait DATA ne sont pas non plus pris en charge par le Département. Il convient donc pour l'utilisateur d'être précautionneux dans ses usages notamment lors de déplacements à l'étranger.

B- 7. Maintenance et Support

La maintenance des matériels ne sera pas assurée par le Département.

Les incidents liés à la synchronisation des matériels personnels seront considérés comme « non prioritaires » par les techniciens de la direction des systèmes d'informations. Le délai de traitement pour régler le problème sera donc non garanti.

B- 8. Sécurité des données

Il est interdit d'enregistrer sur son matériel des informations sensibles (mots de passe, données médicales, données sociales...) afin d'éviter tout risque de fraude, de piratage ou d'usurpation d'identité.

L'utilisateur prend en charge la sécurité de ses données et s'engage à ne pas laisser d'informations professionnelles sur son matériel (documents téléchargés...).

En cas de perte ou de vol :

L'utilisateur changera rapidement le mot de passe de sa messagerie Zimbra.

L'utilisateur avertira dans les meilleurs délais la hotline informatique de la DOSIN afin que celle-ci désactive la synchronisation du mobile ou de la tablette afin d'éviter une usurpation d'identité.

Après son analyse par la DOSIN, en cas de perte de données à caractère personnel ou de suspicion de perte de données, celle-ci avertit la déléguée à la protection des données, laquelle en avisera la CNIL.

Lors de son départ de la collectivité

L'utilisateur en avertira la DOSIN afin qu'elle désactive la synchronisation du mobile.

Utilisation

Le fait de bénéficier de l'accès à sa messagerie professionnelle à partir de son matériel personnel n'autorise pas l'utilisateur à utiliser son matériel à des fins personnelles pendant son temps de travail.

Les données traitées pendant l'utilisation professionnelle de son matériel restent la propriété du Département.

L'utilisation de son matériel personnel lors d'un usage professionnel engage l'utilisateur à respecter le droit d'auteur. Les réalisations effectuées restent la propriété du Département, dans les conditions du code de la propriété intellectuelle, notamment ses articles L111-1 alinéa 3, L121-7-1., L131-3-1 et L131-3-2.

Suppression de la connexion

La DOSIN se réserve le droit de supprimer la connexion du matériel de l'utilisateur sans l'avertir au préalable si elle considère que celle-ci engendre des problèmes de sécurité (non-respect de la règlement relative aux modalités d'utilisation des technologies de l'information et des communications, fuite de données, ...) ou si la direction générale le demande.

Confidentialité des données

S'agissant de son matériel personnel, le Département s'engage à ne collecter/conserver aucune des données de géolocalisation ou autre donnée du matériel de l'utilisateur.

Garantie

En cas de perte, de vol ou de casse de son matériel pendant une utilisation professionnelle, l'utilisateur ne pourra prétendre auprès du Département à aucun remboursement y compris en cas de réparation.

ANNEXE C_Délits pouvant être évoqués en cas de comportement de comportements illicites ou prohibés

Dans ce paragraphe le terme « Contenu numérique » regroupe la consultation ou la contribution sur internet quel que soit le support utilisé (mail, forum, avis, messagerie instantanée...).

C- 1. Consultation et/ou participation à des sites illicites pour laquelle le Département portera plainte contre l'agent qui fera également l'objet d'une procédure disciplinaire.

Par exemple (liste non exhaustive) :

- consultation et/ou participation à des sites pédopornographiques (article 227-23 du code pénal)
- propos tenus sur des sites, forums et par le biais de la messagerie professionnelle relatifs à :
- la provocation publique à la haine, la violence ou la discrimination raciale (article 24 alinéa 7 de la loi du 29 juillet 1881 relative à la liberté de la presse)
- la diffamation publique à raison de l'appartenance ou de la non-appartenance, réelle ou supposée, à une ethnie, une nation, une race ou une religion déterminée (article 29 alinéa 1 et 32 alinéa 2 de la loi du 29 juillet 1881),
- l'injure publique à raison de l'appartenance ou de la non-appartenance, réelle ou supposée, à une ethnie, une nation, une race ou une religion déterminée (article 29 alinéa 2 et 33 alinéa 3 de la loi du 29 juillet 1881),
- la contestation de crime contre l'humanité (article 24 bis de la loi du 29 juillet 1881),
- la provocation non publique à la discrimination, à la haine ou à la violence raciale, nationale ou religieuse (art R.625-7 du code pénal),
- la diffamation non publique raciale, nationale ou religieuse (art R.624-3 du code pénal et 29 alinéa 1 de la loi du 29 juillet 1881),
- l'injure non publique raciale, nationale ou religieuse (art R.624-4 du code pénal et 29 alinéa 2 de la loi du 29 juillet 1881),
- le fait de provoquer directement à des actes de terrorisme ou d'en faire publiquement l'apologie (article 421-2-5 du code pénal).

C- 2. Consultation et/ou participation à des sites prohibés et pour lesquels un agent pourra faire l'objet d'une procédure disciplinaire.

Par exemple (liste non exhaustive) :

- consultation et/ou participation de sites pornographiques, sites de jeux en ligne, ...
- contenus numériques relatifs au prosélytisme (principe de laïcité – article 1er de la Constitution et circulaire PM n° 5209/SG du 13 avril 2007 relative à la Charte de la laïcité dans les services publics) : un tel comportement constitue un manquement à l'honneur qu'implique nécessairement la déontologie du service public, dans la mesure où une telle attitude, par le trouble qu'elle génère, est de nature à instiller, tant dans le service qu'auprès des usagers, un doute non seulement quant à la neutralité de l'intéressé mais également sur celle qui s'attache au service public (Cour administrative d'appel de Nancy, 6 juillet 2006, requête n° 04NC00898).
- contenus numériques ne respectant pas le principe de neutralité (exemple : CE, 15 octobre 2003: même en dehors de tout comportement prosélytique, l'agent sera sanctionné pour manquement au principe de neutralité et à l'obligation de neutralité s'imposant à lui, lorsque, par exemple, il a utilisé les moyens de communication du service au profit d'une association religieuse et qu'il apparaissait sur le site de cette association, en qualité de membre de celle-ci).

Si la consultation et/ou participation aux sites des 1ère et 2e catégories porte atteinte à l'image du Département de la Drôme, la collectivité se réserve la possibilité de porter plainte sur ce fondement contre l'agent en cause.