REPUBLIQUE FRANCAISE

- - - - - - -

Département des Alpes de Haute-Provence

- - - - - - -

Service départemental d'incendie et de secours

Date de convocation : 19 février 2020
Nombre d'élus en exercice : 5
Présents : 3
Absents : 2
Votants : 3
Réception en Préfecture le :
Délibération certifiée exécutoire le :

DELIBERATION N° 2020-25(GRH)

EXTRAIT DU REGISTRE

DES DELIBERATIONS DU BUREAU

DU CONSEIL D'ADMINISTRATION

DU SERVICE DEPARTEMENTAL D'INCENDIE ET DE SECOURS

DES ALPES DE HAUTE-PROVENCE

L'an deux mille vingt et le 25 juin le Bureau du Conseil d'administration du Service départemental d'incendie et de secours s'est réuni au lieu habituel de ses séances, après convocation légale, sous la présidence de Monsieur Pierre POURCIN.

Etaient présent(e)s : Monsieur Robert GAY, 1er vice-président ; monsieur Serge SARDELLA, membre du Bureau.
Etaient excusé(e)s : Madame Geneviève PRIMITERRA, 2ème vice-présidente, monsieur Bernard DIGUET, 3ème vice-président.

Objet : Adoption de la charte informatique :

Le Président POURCIN expose :

Le 25 mai 2018, le règlement européen concernant la RGPD est entré en application. De nombreuses formalités auprès de la CNIL disparaissent. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

La CNIL préconise de préparer la RGPD en plusieurs étapes. La rédaction et la promulgation des chartes informatiques à destination des administrateurs réseaux, des utilisateurs et agents publics ainsi que du guide utilisateurs participe à l'étape qui a pour but d'organiser les processus internes.

Définition selon la CNIL sur l'organisation des processus internes : « *Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire).* »

Vous trouverez en annexe au présent rapport :

- La charte de l'administrateur,
- La charte de l'utilisateur,
- Le guide de l'utilisateur.
-

Le comité technique, lors de sa séance du 11 juin 2020, a donné un avis favorable à l'unanimité.
Il est demandé aux membres du Bureau de bien vouloir en délibérer.

Après en avoir délibéré le Bureau du Conseil d'administration a adopté ce rapport à l'unanimité.

Le Président du Conseil d'administration

Pierre POURCIN

sdis sapeurs pompiers
Alpes de Haute-Provence

CHARTE DE L'ADMINISTRATEUR

MARS 2020 > V 3.0

SOMMAIRE

1 Approche générale

1.1 Préambule

Les administrateurs de système d'information (ci-après les « administrateurs ») peuvent selon leurs habilitations être affectés à un certain nombre de missions comme :

- la gestion, l'exploitation et la maintenance du système d'information de l'établissement ;
- le suivi et le contrôle de l'utilisation des ressources informatiques ;
- la mise en œuvre des logiciels et autres applications.

A cet égard, ils peuvent être amenés à avoir accès à certaines informations ou données d'autres utilisateurs, données présentant, par ailleurs, un caractère confidentiel.

La présente charte est rédigée dans l'intérêt des administrateurs et manifeste la volonté de l'établissement d'assurer un développement harmonieux et sécurisé des ressources informatiques.

L'administrateur s'engage à respecter les termes de la présente charte.

1.2 Objet

La présente charte a pour objet de formaliser les principales prérogatives des administrateurs, ainsi que les principales obligations qui pèsent sur eux dans le cadre de l'exercice de leurs fonctions.

1.3 Référentiel

La présente charte prend place au sein d'un référentiel qui se compose de la manière suivante :

- la présente charte de l'administrateur ;
- la charte de l'utilisateur ;
- la charte des tiers ;
- le guide de l'utilisateur énonçant de manière non exhaustive les principales dispositions légales applicables ;
- le livret des procédures de sécurité.

1.4 Définitions

Au sens de la présente charte, les termes ci-dessous ont la signification suivante :

- « administrateur » : personne spécialement compétente en matière informatique, qui doit veiller à assurer le fonctionnement normal et la sécurité des ressources informatiques ou qui dispose de droits d'accès privilégiés sur tout ou partie du système d'information dont il n'est pas que l'utilisateur ;
- « charte des tiers » : formalisation des règles s'appliquant à toute personne autorisée à accéder et à utiliser les moyens informatiques mis à disposition par la société, en exécution d'un contrat autre qu'un contrat de travail, et ce quel que soit son statut ;
- « charte de l'utilisateur » : formalisation des principales mesures de contrôle mises en œuvre par la société dans le cadre de l'utilisation des ressources informatiques par les utilisateurs ;
- « correspondant chartes » : interlocuteur privilégié des utilisateurs des administrateurs et des tiers dans le cadre de la mise en œuvre de la charte de l'utilisateur, de la charte de l'administrateur et de la charte des tiers ;
- « donnée à caractère personnel » : toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ;

- « guide de l'utilisateur » : document exposant aux utilisateurs les principales règles juridiques applicables dans le cadre de l'utilisation des ressources informatiques de de l'établissement ;
- « livret des procédures de sécurité » : document à caractère technique permettant l'implémentation pratique des dispositions figurant dans la charte de l'utilisateur ;
- « ressources informatiques » : ensemble des moyens matériels, logiciels informatiques (ordinateurs fixes, ordinateurs portables, clés USB, CD-Rom, DVD-Rom, PDA, appareils photos, etc.), de communications électroniques et de télécommunications (téléphonie, messagerie électronique, internet, intranet, etc.) mis à disposition des utilisateurs pour des utilisations internes (Intranet) et externes (Internet et réseaux privés ou publics de communications électroniques) ;
- « système d'informations » : système de traitement de l'information et de télécommunications de de l'établissement, qui fournit et distribue des informations et permet via les moyens informatiques et/ou de télécommunications, de les constituer, créer, échanger, diffuser, dupliquer, reproduire, stocker et détruire ;
- « utilisateur » : toute personne autorisée à utiliser les ressources informatiques de l'entreprise, et ce quel que soit son statut : salariés, personnel intérimaire, stagiaires, personnel des prestataires extérieurs intervenant dans le cadre d'un contrat de sous-traitance, ainsi que les consultants.

1.5 Champ d'application

La présente charte s'applique aux administrateurs, qu'il s'agisse :

- des administrateurs internes, membres du Service Transmissions, Informatique et Téléphonie du SDIS 04 ;
- des administrateurs externes, prestataires de services extérieurs intervenant dans le cadre d'un contrat de sous-traitance.

2 Prérogatives des administrateurs

2.1 Missions à titre préventif

A des fins de sécurité et de fonctionnement optimal du système d'information, l'administrateur assure, dans le cadre des missions qui lui sont confiées et sur la base des instructions données par le Service Transmissions, Informatique et Téléphonie :

- la gestion des traces et des logs du système d'information et veille à cet égard à leur durée de conservation conformément aux dispositions légales en vigueur ;
- la mise en place d'une politique sécuritaire ayant pour objet d'assurer la sécurité technique du système d'information ;
- la sécurité, la confidentialité et la sauvegarde des données ;
- la veille et la mise à jour systématique des logiciels et/ou des outils assurant la sécurité du système d'information et notamment des anti-virus ;
- la continuité du service du système d'information ;
- la maintenance préventive du système d'information.

Par ailleurs, l'administrateur se voit reconnaître la possibilité d'accéder :

- concernant la téléphonie fixe, aux six derniers chiffres correspondant aux numéros entrant et sortant ;
- concernant la téléphonie mobile dont l'usage est exclusivement professionnel, aux dix chiffres des numéros entrant et sortant.

2.2 Missions à titre curatif

Dans tous les cas où l'administrateur aura constaté un dysfonctionnement du système d'information ou un manquement par un utilisateur à l'une des règles d'usage et de sécurité des ressources informatiques, il s'engage :

- s'il s'agit d'un administrateur interne, à informer immédiatement l'autorité hiérarchique dont il dépend et le Service Transmissions, Informatique et Téléphonie ;
- s'il s'agit d'un administrateur externe, à informer immédiatement le Service Transmissions, Informatique et Téléphonie.

Dans ces conditions, l'administrateur n'interviendra pour faire cesser ce dysfonctionnement ou ce manquement que sur les instructions du Service Transmissions, Informatique et Téléphonie.

En cas de force majeure ou en cas de mesure d'urgence, l'administrateur peut intervenir seul et prendre les mesures nécessaires au maintien de la sécurité, à la sauvegarde et au bon fonctionnement du système d'informations. Il en informe la direction des systèmes d'informations dans les meilleurs délais.

2.3 Prise en main à distance

L'administrateur peut, dans le cadre des missions qui lui sont confiées, recourir à des outils de prise en main à distance des postes informatiques des utilisateurs, notamment à des fins de maintenance informatique.

Dans cette hypothèse, l'administrateur s'interdit d'utiliser ces outils pour exercer un contrôle de l'activité des utilisateurs et, en tout état de cause, les utilisera dans les strictes limites de ses missions.

L'administrateur s'engage ainsi à n'accéder qu'aux données nécessaires à l'accomplissement de ses missions et à en assurer la confidentialité.

L'utilisateur sera informé de cette prise de main à distance par un message d'information apparaissant sur son écran. Sans la validation du message d'information par l'utilisateur, la personne habilitée en charge de la maintenance ne pourra intervenir.

3 Obligations des administrateurs

3.1 Obligation de confidentialité

L'administrateur s'engage à respecter une confidentialité absolue du contenu des données, fichiers, traitements et informations dont il pourrait avoir connaissance dans le cadre de l'exercice de ses missions.

A cet égard, l'administrateur s'engage à garder confidentielles et à ne pas divulguer à des tiers toutes informations qui lui ont été révélées ou dont il a eu connaissance.

Concernant les fichiers, données et messages à caractère privé (désignés « PRIVE » ou « Privé ») des utilisateurs pouvant être contenus dans tout ou partie du système d'informations, l'administrateur s'engage à tout mettre en œuvre pour ne pas y accéder. Dans l'hypothèse où il y accéderait néanmoins, il s'engage à en assurer la confidentialité et l'intégrité dans les conditions de la présente charte.

L'administrateur s'engage à prendre toutes les mesures de sécurité nécessaires à la protection des informations et au maintien de leur confidentialité absolue.

L'administrateur s'engage à respecter la plus stricte confidentialité des mots de passe des utilisateurs.

3.2 Obligation de respecter les droits des tiers

Dans le cadre de l'exercice de ses missions, l'administrateur s'engage à ne pas porter atteinte :

- au droit des utilisateurs au respect de leur vie privé dans le cadre de l'utilisation des ressources informatiques de de l'établissement ;
- aux droits de propriété intellectuelle des tiers, notamment dans le cadre du téléchargement de logiciels ou bases de données sécuritaires. Les logiciels doivent être utilisés dans les conditions de licences souscrites par la société. Toutes les créations de tiers protégés par le droit d'auteur (logiciel, bases de données, etc.) ne doivent pas être reproduits, utilisés, copiées ou remises à des tiers sans autorisation.

3.3 Obligation de respecter la loi Informatique et libertés

Dans le cadre de l'exercice de ses missions, l'administrateur s'engage à respecter les dispositions de la loi Informatique et Libertés du 6 janvier 1978 modifiée et notamment à ne réaliser aucun traitement de données à caractère personnel sans l'accord expresse de la direction des systèmes d'information et la réalisation le cas échéant des formalités préalables auprès de la Cnil.

L'administrateur s'engage à assurer la sécurité et la confidentialité des données à caractère personnel figurant dans les fichiers appartenant à la société.

3.4 Obligation d'information, de conseil et d'alerte

L'administrateur s'engage à informer la direction des systèmes d'informations des modalités et éventuelles difficultés de mise en œuvre de la politique de sécurité.

L'administrateur informe d'urgence la direction des systèmes d'informations et/ou l'autorité hiérarchique dont il dépend de toute alerte technique et de toute situation d'urgence rencontrée relative au système d'informations.

Il se tient à la disposition de toute autorité compétente et en particulier de toute autorité judiciaire et l'informe, ainsi que la direction des systèmes d'information, des contenus illicites, notamment pédo-pornographiques ou diffamatoires qu'il constaterait.

L'administrateur s'engage à une obligation générale de conseil, d'information, de recommandation, d'alerte et de mise en garde auprès de l'autorité hiérarchique dont il dépend et du responsable de la sécurité des systèmes d'informations.

En outre, l'administrateur assure une veille générale du système d'informations et informe le responsable de la sécurité des systèmes d'information et/ou l'autorité hiérarchique dont il dépend de tout dysfonctionnement qu'il pourrait constater.

3.5 Obligation de tenir le registre de traitement

L'administrateur est tenu de renseigner et tenir à jour le registre de traitement.

4 Sanctions

Le non-respect de tout ou partie des dispositions figurant dans la présente charte pourra entraîner pour l'administrateur l'application de sanctions disciplinaires et/ou la mise en œuvre d'une procédure judiciaire.

5 Evolution de la charte

L'administrateur destinataire de la présente charte est invité à transmettre à la direction des systèmes d'informations toute proposition de modification ou d'ajout dont il a pu constater l'intérêt dans le cadre de sa mission d'administrateur.

La présente charte sera régulièrement mise à jour et sera portée à la connaissance des administrateurs sur support papier ou électronique.

Dans l'hypothèse où la charte mise à jour serait portée à la connaissance des administrateurs par voie électronique, l'acceptation de la charte modifiée sera réalisée en ligne par chaque administrateur dûment identifié au moyen de son identifiant et de son mot de passe et selon la procédure de double clic ayant la même valeur qu'une signature manuscrite. La version de la charte modifiée acceptée par l'administrateur (et les données d'identification) sera conservée dans des conditions permettant d'en garantir l'intégrité et sera considérée comme la preuve de l'acceptation de l'administrateur des dispositions de la charte modifiée.

6 Publicité

La présente charte et ses mises à jour seront publiées sur l'intranet.

7 Acceptation de la charte

L'administrateur par sa signature de la présente charte reconnaît avoir lu et déclare avoir compris la présente charte et les règles déontologiques et de sécurité auxquelles il est également soumis.

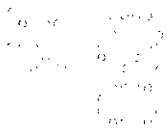
L'administrateur s'engage à respecter la présente charte lors de tout accès au système d'informations

Nom :

Qualité :

Date :

Signature :



sdis sapeurs pompiers
Alpes de Haute-Provence

CHARTE UTILISATEUR RELATIVE AUX AGENTS PUBLICS

MARS 2020 > V 3.0

SOMMAIRE

1 Préambule

Le SDIS 04 met à la disposition de ses agents publics, ci-après dénommés « les utilisateurs », des ressources informatiques nécessaires à l'accomplissement de leurs missions.

L'utilisation des ressources informatiques suppose le respect par les utilisateurs des règles destinées à assurer un niveau optimum de sécurité, de confidentialité de performance et, d'une manière générale, le respect des dispositions légales et réglementaires applicables et notamment du régime statutaire et réglementaire de la fonction publique.

La présente charte est rédigée dans l'intérêt des utilisateurs et manifeste la volonté de l'établissement d'assurer un développement harmonieux et sécurisé de l'accès et de l'utilisation des ressources informatiques.

La présente charte illustre le comportement loyal, respectueux et responsable que chacun doit observer à l'occasion de l'utilisation des ressources informatiques de l'établissement.

2 Objet

La présente charte a pour objet de formaliser les principales règles en matière d'utilisation et de sécurité des ressources informatiques.

La présente charte a également pour objet de formaliser les principales mesures de contrôle mises en œuvre par l'établissement, dans le cadre de l'utilisation des ressources informatiques par les utilisateurs.

La présente charte est complétée par un guide qui a pour objet d'exposer aux utilisateurs les principales règles juridiques applicables dans le cadre de l'utilisation des ressources informatiques de l'établissement et par un livret des procédures de sécurité définissant les principales règles techniques et pratiques de mise en œuvre des règles générales et permanentes figurant dans la présente charte.

3 Opposabilité de la charte

La charte a été portée à la connaissance des utilisateurs et est entrée en vigueur dans les conditions fixées par l'article « Entrée en vigueur » de la présente charte.

4 Définitions

Au sens de la présente charte, les termes ci-dessous ont la signification suivante :

- « administrateur » : personne spécialement compétente en matière informatique, qui doit veiller à assurer le fonctionnement normal et la sécurité des ressources informatiques ou qui dispose de droits d'accès privilégiés sur tout ou partie du système d'information dont il n'est pas que l'utilisateur. Les administrateurs sont également soumis à la charte de l'administrateur ;
- « charte de l'administrateur » : formalisation des règles et procédures de sécurité propres aux administrateurs ;
- « charte des tiers » : formalisation des règles s'appliquant à toute personne autorisée à accéder et à utiliser les moyens informatiques mis à disposition par le SDIS 04, en exécution d'un contrat autre qu'un contrat de travail, et ce quel que soit son statut ;
- « correspondant chartes » : interlocuteur privilégié des utilisateurs, des administrateurs et des tiers dans le cadre de la mise en œuvre de la charte de l'utilisateur, de la charte de l'administrateur et de la charte des tiers ;
- « donnée à caractère personnel » : toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres
- « guide de l'utilisateur » : document exposant aux utilisateurs les principales règles juridiques applicables dans le cadre de l'utilisation des ressources informatiques du SDIS 04 ;

- « livret des procédures de sécurité » : document à caractère technique permettant l'implémentation pratique des dispositions figurant dans la charte ;
- « matériel nomade » : moyens techniques, tels que notamment ordinateurs portables, assistants personnels, téléphones mobiles et éléments accessoires (CD-Rom, DVD-Rom, clés USB, équipements réseaux, équipements sans fil, dispositifs de communication à distance) mis à disposition de l'utilisateur et pouvant être utilisés à l'extérieur du SDIS 04 ;
- « messagerie » : tout courrier au format électronique transmis à l'aide des services informatiques mis à disposition ;
- « peer to peer » : procédé d'échange de fichiers électroniques directement entre des postes individuels d'utilisateurs connectés à Internet ;
- « ressources informatiques » : ensemble des moyens matériels, logiciels informatiques (ordinateurs fixes, ordinateurs portables, Smartphones, tablettes, clés USB, CD-Rom, DVD-Rom, appareils photos, etc.), de communications électroniques et de télécommunications (téléphonie, messagerie électronique, internet, intranet, etc.) mis à disposition des utilisateurs pour des utilisations internes (intranet) et externes (internet et réseaux privés ou publics de communications électroniques) ;
- « système d'informations » : système de traitement de l'information et de télécommunications du SDIS 04, qui fournit et distribue des informations et permet via les moyens informatiques et/ou de télécommunications, de les constituer, créer, échanger, diffuser, dupliquer, reproduire, stocker et détruire ;
- « utilisateur » : toute personne autorisée à utiliser les ressources informatiques du SDIS 04, et ce quel que soit son statut : salarié, agent public, personnel intérimaire, stagiaire, personnel des prestataires extérieurs intervenant dans le cadre d'un contrat de sous-traitance, ainsi que les consultants.

5 Champ d'application

La présente charte s'applique à tous les utilisateurs des ressources informatiques mis à disposition par l'établissement.

5.1 Utilisateurs

Les membres de la direction des systèmes d'information sont, en leur qualité d'utilisateurs, soumis au respect de la présente charte. Ils sont également soumis, en leur qualité d'administrateurs, au respect d'une charte complémentaire dénommée « charte de l'administrateur ».
Les représentants du personnel et les membres des organisations syndicales sont, en leur qualité d'utilisateurs, soumis au respect de la présente charte. En revanche, l'accès aux ressources informatiques et leur utilisation, dans le cadre de l'exercice de leurs activités de représentation ou syndicales, sont subordonnés à la signature d'un accord d'entreprise.

5.2 Ressources informatiques

L'ensemble des ressources informatique, mises à la disposition des utilisateurs sont et demeurent la propriété de l'établissement.

L'utilisateur peut également, s'il le souhaite, faire usage de l'ensemble des moyens de communications électroniques qui sont sa propriété personnelle et pour lesquels il a obtenu une autorisation d'utilisation dans le cadre de son activité professionnelle.

Dans le cas d'une utilisation par l'utilisateur de moyens de communications électroniques qui sont sa propriété personnelle, ces moyens sont soumis à la présente charte.

5.3 Usages concernés

La présente charte s'applique à tous les types d'usage qu'ils aient lieu :

- dans les locaux de l'établissement ;
- dans le cadre d'un usage dit « nomade », quel que soit le lieu ;
- dans le cadre d'un accès distant, quel que soit le lieu de cet accès (domicile, etc.).

La présente charte s'applique quelles que soient la fréquence et la périodicité de l'utilisation des moyens informatiques et de communications électroniques.

6 Organisation interlocuteurs

La mise en œuvre de la présente charte intervient dans le cadre de l'organisation suivante :

- l'autorité hiérarchique dont dépend l'utilisateur concerné ;
- le correspondant chartes ;
- la direction des systèmes d'information.

Toute demande d'un utilisateur relative à l'application ou à l'interprétation de la présente charte, du guide de l'utilisateur et du livret des procédures de sécurité doit être adressée au correspondant chartes.

7 Règles d'utilisation et de sécurité des ressources informatiques

7.1 Règles générales

7.1.1 Accès et identification

L'accès aux ressources informatiques nécessite une autorisation préalable (l'attribution d'un droit d'accès) et passe par l'affectation d'un identifiant et d'un mot de passe.
Ce droit d'accès peut être différent d'un utilisateur à l'autre selon le profil attribué, lequel profil est attribué en considération du statut, de la mission, de la nature du poste et des besoins professionnels.
Ce droit d'accès est personnel et non cessible : l'identifiant et le mot de passe doivent être protégés et ne doivent pas être divulgués.
Il appartient à l'utilisateur de choisir un mot de passe sûr, étant précisé que l'efficacité du mot de passe dépend du nombre de caractères alphanumériques tel que défini au livret des procédures de sécurité, de son originalité, de son renouvellement selon la fréquence établie par la direction des systèmes d'information.
L'utilisateur s'interdit d'utiliser un identifiant et/ou un mot de passe autre que le sien et s'interdit d'user de son identifiant et /ou de son mot de passe pour accéder à des applications, des données ou un compte informatique autres que ceux qui lui auront été éventuellement attribués ou pour lesquels il a reçu l'autorisation d'accès.
L'utilisateur est responsable de l'utilisation qui est faite de son droit d'accès : sauf si une mesure de suppression ou de suspension a été engagée, pour quelle que raison que ce soit, tout usage des ressources informatiques est réputé avoir été réalisé par le titulaire du droit d'accès, qui assume les conséquences juridiques et financières de tout usage fautif.

Le droit d'accès cesse automatiquement lors d'un départ (l'utilisateur quittant l'établissement) ou lors d'un changement d'affectation (changement de poste, mutation, etc.) ou s'il est constaté que l'utilisateur a violé l'une des obligations imposées par la présente charte.

La direction des systèmes d'information peut interrompre, modifier ou supprimer à tout utilisateur l'accès à tout ou partie des ressources informatiques, pour quelle que raison que ce soit, de manière temporaire ou définitive, générale et non discriminatoire et ce, sans qu'elle ne puisse être tenue responsable des conséquences de sa décision.

La direction des systèmes d'information s'efforcera, autant que faire se peut, de prévenir les utilisateurs dans des délais raisonnables.

Les modalités de gestion des mots de passe, des droits d'accès et les contrôles d'accès sont plus amplement décrites au livret des procédures de sécurité.

7.1.2 Utilisation professionnelle / personnelle

Les ressources informatiques sont mises à la disposition de l'utilisateur, selon le profil qui lui a été attribué.

Les ressources informatiques sont réservées à un usage professionnel.
Toutefois, une utilisation des ressources informatiques à des fins personnelles est admise dans les limites définies par la présente charte. En toute hypothèse, l'utilisation à des fins personnelles des ressources informatiques est limitée à un usage raisonnable ; il ne doit pas, en aucune manière, perturber le bon fonctionnement du service et des ressources informatiques. En revanche, toute utilisation personnelle des ressources informatiques à des fins lucratives est interdite.

Il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé (messages, lettres, etc....) dans l'hypothèse où il en disposerait, dans un répertoire de données situé exclusivement sur son poste de travail nommé « Privé » ou « PRIVE » et ce, conformément aux dispositions de l'article «Messages privés / répertoires privés » de la présente charte.

Il appartient à l'utilisateur de veiller à ce que les messages à caractère privé comportent dans leur objet la mention « Privé » ou « PRIVE » conformément aux dispositions de l'article « Messages privés / répertoires privés ». A défaut de la mention « Privé » ou « PRIVE » les échanges électroniques sont considérés comme des échanges de nature professionnelle.

7.1.3 Utilisation interdite des moyens informatiques et de communications électroniques

Il est notamment interdit sans que cette liste soit exhaustive de :

- envoyer des messages à caractère injurieux, dénigrant, diffamatoire, dégradant ou susceptibles de porter atteinte à la vie privée des personnes ou à leur dignité, relatifs à la race, l'origine ethnique, les mœurs, la religion, les opinions politiques, les origines sociales, l'âge ou le handicap ; en cas de réception de tels messages, l'utilisateur doit les supprimer dans les meilleurs délais, après avoir informé la direction des systèmes d'information ;

- consulter, copier ou télécharger le contenu de fichiers ou de sites à caractère pornographique, pédopornographique, négationniste, extrémiste ou contraire aux bonnes mœurs ou à l'ordre public tels que notamment la pornographie, la pédopornographie et plus généralement tous comportements répréhensibles. Ces actes peuvent revêtir le caractère d'une infraction pénale qui pourra être dénoncée à qui de droit ;
- adopter tout comportement pouvant inciter des tiers à adresser à l'utilisateur de tels documents sous forme d'informations, d'images, de vidéos, de fichiers, etc ;
- utiliser les ressources de l'entreprise à des fins de harcèlement, menace, chantage et, de manière générale, à violer des droits en vigueur ;
- falsifier le contenu et les propriétés d'un fichier ;
- utiliser l'identité d'un tiers à des fins autres que celles pour lesquelles l'utilisateur a été autorisé ;
- créer des pages Web personnelles ;
- diffuser l'adresse de courrier électronique professionnelle sur des sites Internet sans rapport avec l'activité professionnelle ;

- participer à des chaînes de courrier électronique ;
- commettre toute action susceptible de mettre en cause la sécurité matérielle ou juridique du SDIS 04 et de porter atteinte à sa réputation ;
- porter atteinte au système d'information du SDIS 04 ou de toutes autres organisations ;
- commettre toute action impliquant :

    - tout mode de chiffrement non conforme aux procédures internes, sauf dérogation expresse de la direction des systèmes d'information ;
    - la dissimulation de l'identité par utilisation de pseudonymes ;
    - et plus généralement toute action illégale, contraire à la charte ou aux procédures applicables et toute action susceptible d'entraîner la responsabilité civile ou pénale de l'entreprise.

7.1.4 Gestion des absences

Chaque utilisateur doit veiller, en cas d'absence temporaire, à ce que la continuité du service soit assurée, conformément aux modalités d'organisation du service et telle que définie par la hiérarchie.

Chaque utilisateur doit ainsi veiller à indiquer ses périodes d'absence à son supérieur hiérarchique et à ses interlocuteurs habituels, et mettre en place les mesures de gestion d'absence visées à l'article « Consultation de la messagerie électronique » de la présente charte.

L'utilisateur est en outre informé qu'en cas d'absence, l'établissement peut être contraint d'accéder, dans le respect de la vie privée de l'utilisateur, et pour les besoins de la continuité de l'activité de l'établissement aux données stockées sur son poste de travail (fichiers, messageries, support de stockage).

Il appartient à l'utilisateur de communiquer sur demande de son supérieur hiérarchique tout identifiant et/ou mot de passe au correspondant chartes.

Par ailleurs, en cas de suspension du contrat de travail, l'utilisateur s'interdit d'utiliser les ressources informatiques, les accès de l'utilisateur pouvant être désactivés pendant la durée de cette absence et ce, à l'initiative de l'autorité hiérarchique dont il dépend.

Les modalités de gestion des absences concernant la messagerie électronique sont décrites ci-après.

7.1.5 Gestion des départs

Lors de son départ de l'établissement, l'utilisateur doit remettre à sa hiérarchie l'ensemble des ressources informatiques mis à sa disposition et ce, en bon état de fonctionnement.

Le droit d'accès de l'utilisateur est alors désactivé pendant 30 jours et supprimé après 30 jours.

Si l'utilisateur a bénéficié d'un moyen d'authentification à distance, il s'engage à le restituer.

Il appartient par ailleurs à l'utilisateur de détruire son répertoire «privé», lors de son départ de l'établissement. S'il n'a pas été détruit par ce dernier au jour de son départ, il sera supprimé par l'établissement sans copie ni prise de connaissance préalable du contenu.

Sauf nécessité liée à la continuité du service le départ d'un utilisateur entraîne la fermeture de sa boite aux lettres électronique au jour de son départ. Il est de la responsabilité de

l'utilisateur, de faire suivre ses messages à caractère privé en communiquant sa nouvelle adresse à ses interlocuteurs, et de supprimer ses messages à caractère privé de sa boite aux lettres électronique.

7.1.6 Sécurité

7.1.6.1 Politique générale

L'utilisateur s'engage à user des ressources informatiques de façon loyale et dans le respect de la présente charte et des dispositions légales et réglementaires en vigueur.

L'utilisateur s'engage à contribuer activement à la sécurité générale et à assurer la confidentialité et la conservation de toutes les données auxquelles il a accès, et ce en utilisant les moyens mis à sa disposition et sur la base des instructions qui lui ont été données par l'autorité hiérarchique dont il dépend et celles figurant dans les procédures de maintenance et d'utilisation.

A cet égard, l'utilisateur s'engage à :

- ne transmettre aucune information confidentielle sans l'autorisation d'un supérieur hiérarchique ;
- veiller à ce que les tiers non autorisés n'aient pas connaissance d'une telle information ;
- ne transmettre en tout état de cause aucune information à caractère professionnel sous la forme d'un message à caractère privé ;
- ne transmettre en tout état de cause aucune information à caractère professionnel au moyen d'une autre messagerie que celle mise à sa disposition par l'établissement ;
- ne pas rechercher ni ouvrir un message qui ne lui est pas adressé sans l'autorisation de son destinataire, à l'exclusion du supérieur hiérarchique ;
- ne pas utiliser, sans l'accord de l'utilisateur concerné, les ressources informatiques qui sont affectées à ce dernier ;
- ne pas installer, télécharger ou utiliser sur les équipements informatiques de l'établissement des logiciels et/ ou progiciels sans qu'une licence d'utilisation appropriée n'ait été souscrite par l'établissement et en particulier ne pas télécharger de logiciel de partage de données sur Internet tels que notamment des logiciels de type « peer to peer » ;
- ne pas porter atteinte aux droits de propriété intellectuelle d'un tiers ni aux mesures de protection mises en œuvre par l'établissement, notamment les ressources informatiques ne doivent en aucune manière être utilisées 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, photographies, œuvres musicales, œuvres audiovisuelles, logiciels et jeux vidéo, sans l'autorisation des titulaires des droits prévus aux livres I et II du Code de la propriété intellectuelle lorsque cette autorisation est requise ;
- ne pas détenir, offrir, céder ou mettre à disposition, un équipement, un programme informatique permettant :
- d'accéder ou de se maintenir frauduleusement dans un système de traitement automatisé ;
- d'entraver ou de fausser le fonctionnement système de traitement automatisé ;
- d'introduire frauduleusement des données dans un système de traitement automatisé ;
- ne pas télécharger, accéder ou tenter d'accéder à des ressources, fichiers ou programmes pour lesquels l'utilisateur ne bénéficie pas d'une habilitation expresse de l'autorité hiérarchique dont il dépend ;
- ne pas installer de périphérique non fourni par l'établissement ;

- ne pas stocker sur des espaces autres que ceux dédiés par l'établissement des informations à caractère professionnel ;
- d'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, les obligations de réserve et le devoir de discrétion en usage au sein de l'établissement.

En cas d'absence prolongée (au-delà d'une heure), l'utilisateur s'engage à fermer ou mettre en veille les documents et les sessions en cours. Il ne doit pas quitter son poste de travail, ni ceux en libre-service sans se déconnecter, ou mettre en veille, en laissant les moyens et services internes accessibles.

L'utilisateur s'engage à être vigilant en signalant toute anomalie ou intrusion. L'utilisateur est tenu d'informer, sans délai, sa hiérarchie de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les ressources informatiques et leur contenu.

En cas de fraude informatique ou dans toute autre hypothèse où l'utilisateur serait invité à prendre des mesures d'urgence ou de sécurité spécifique, celui-ci s'engage à les appliquer sans le moindre délai.

7.1.6.2 Dispositif de lutte contre les virus informatiques

L'utilisateur doit se conformer au dispositif de lutte contre les virus informatiques tel que décrit dans la présente charte et dans le livret des procédures de sécurité.

A ce titre, l'utilisateur s'engage notamment à :

- ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du message est inconnu ;
- détruire les messages du type « chaîne de solidarité » ;
- ne pas stocker et router des fichiers illégaux, des gadgets reçus ou trouvés sur internet ;
- ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir la direction des systèmes d'information ou l'autorité hiérarchique dont il dépend.

L'utilisateur s'interdit en outre de :

- modifier ou détruire, ou tenter de modifier ou détruire, des fichiers sur lesquels il ne dispose d'aucun droit, en particulier les fichiers contenant des informations comptables ou d'identification ;
- mettre à la disposition d'utilisateurs non autorisés un accès au système d'informations à travers les matériels dont il a usage ;
- procéder à des échanges de fichiers sur internet permettant l'accès à des tiers à tout ou partie du disque dur du SDIS 04, par exemple au moyen d'un logiciel de type « peer to peer » ;
- utiliser ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués, ou masquer son identité ;
- effectuer des opérations pouvant nuire aux relations internes ou externes du SDIS 04.

7.1.7 Traçabilité et filtrage

Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité à :

- apporter la preuve, le cas échéant, du bon usage des moyens informatiques et de communications électroniques mis à la disposition des utilisateurs ;
- prévenir tout usage illicite de ces mêmes moyens.

Le SDIS 04 procède, dans le respect de l'information des personnes concernées et de la loi Informatique et libertés du 6 janvier 1978 modifiée à la mise en place :

- d'outils de traçabilité ;
- d'outils de filtrage.

Dans le respect des principes de transparence et de proportionnalité, l'attention des utilisateurs est attirée sur le fait que les dispositifs de sécurité informatique (pare-feu, systèmes de contrôle des accès, etc.) mis en place par le SDIS 04 enregistrent des traces.

L'utilisateur est donc informé que les messages qu'il émet ou reçoit sont conservés, de même que notamment les traces suivantes :

- date et heure des authentifications de l'utilisateur sur le système d'accès au système d'information ;
- liste des ressources du système d'information auxquelles l'utilisateur a eu accès sur Internet avec les paramètres techniques de connexion, notamment identifiant de compte de l'utilisateur, date et heure, volume des données transmises ;
- liste des paramètres techniques nécessaires à la gestion des services de messagerie électronique : identification du compte de l'utilisateur, coordonnées du destinataire, date et heure, volume, format et nature des pièces jointes.

Les traces et messages pourront être conservés pendant une durée maximale de six mois, sauf si des dispositions légales ou réglementaires venaient à imposer aux établissements des délais de conservation plus longs.

Les utilisateurs sont informés que des systèmes de filtrage sont mis en place, en particulier :

- pour les messages entrants et sortants avec un contrôle antiviral ;
- pour les messages dont la taille ou la liste de destinataires est trop importante ;
- pour les messages en provenance ou à destination d'un utilisateur ou d'un serveur de messagerie électronique de nature manifestement hostile (envoi massif de messages, harcèlement d'un utilisateur, etc.) ;
- pour bloquer, sur la base d'une liste de mots-clés des messages ou l'accès à des sites non autorisés ;
- plus généralement, tout filtrage nécessaire pour préserver la sécurité du système d'information peut être mis en œuvre.

Le fonctionnement de ces systèmes de filtrage ressort de la compétence des administrateurs.

7.2 Transmission des informations et chiffrement

La transmission de données confidentielles ne peut être réalisée qu'aux conditions suivantes :

- habilitation de l'émetteur ;
- désignation d'un destinataire autorisé ;
- respect d'une procédure sécurisée.

L'utilisation de procédés de chiffrement est une fonction qui ne peut être mise en œuvre que dans certains cas autorisés. Il est interdit d'utiliser des moyens de chiffrement autres que ceux expressément autorisés par le SDIS 04.

7.3 Mesures d'urgence et plan de continuité d'activité

L'utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, le SDIS 04 peut mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la continuité de son activité et le respect de ses engagements contractuels ou légaux.

Dans cette hypothèse, l'utilisateur pourra être amené à la demande du SDIS 04 à prendre des mesures d'urgence et de sécurité spécifiques, qu'il s'engage à appliquer sans délai.

Ces mesures exceptionnelles peuvent inclure, notamment, une dégradation de service sur tout ou partie des ressources du système d'informations (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information, etc.), la suppression temporaire de l'accès à certaines ressources du système d'informations (messagerie, connexion internet, accès applicatifs, éléments relatifs au poste de travail, etc.) ou la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au site ou au système d'informations, télétravail, déplacement sur des sites de secours tiers, etc.).

7.4 Equipements informatiques

7.4.1 Dispositions générales

Sauf disposition expresse contraire, une utilisation à des fins personnelles des équipements informatiques est admise.

Les équipements informatiques, mis à disposition de l'utilisateur, sont exclusivement installés, configurés et paramétrés par le personnel habilité de la direction des systèmes d'information.

En toute hypothèse, l'utilisateur s'interdit :

- de modifier ces équipements pas l'ajout de logiciels et matériels n'appartenant pas à l'établissement ;
- dans le cas où des logiciels et/ou matériels lui sembleraient nécessaires pour l'exercice de sa mission, il en fait la demande à sa hiérarchie ;
- l'ajout de matériels ou logiciels ne présentant une nécessité réelle pour l'exercice des missions confiées ou de nouvelles missions ne pourra pas recevoir un avis favorable du Service Transmissions-Informatique-Téléphonie.
- de désactiver les programmes antivirus installés sur les équipements informatiques.

Par ailleurs, l'utilisateur s'engage à réaliser des sauvegardes périodiques.

7.4.2 Equipements nomades

Par équipements informatiques nomades, il faut entendre tous les moyens techniques (ordinateurs portables, Smartphones, tablettes, etc.) et tous les moyens accessoires (clés USB, CD-Rom, etc.) qui peuvent être utilisés hors les murs de l'établissement.

Les équipements informatiques nomades sont remis à l'utilisateur contre récépissé.

L'usage des équipements informatiques nomades est limité à un usage strictement professionnel.

L'utilisateur a parfaitement conscience des conséquences préjudiciables qui pourraient résulter de la perte de ces équipements, de leur soustraction frauduleuse par autrui ou de

l'accès par un tiers à leur contenu : perte financière, perte ou fuite d'informations ou données présentant un caractère confidentiel etc.

Compte tenu de ce qui précède, l'utilisateur s'engage à :

- mettre systématiquement les équipements sous clef, en cas d'absence ;
- ne pas les laisser, sans surveillance, à la vue d'autrui ;
- ne pas stocker les sauvegardes (CD Rom etc.) réalisées à proximité des équipements.

Par ailleurs, l'attention de l'utilisateur est attirée sur les risques d'intrusion par un tiers dans le système informatique de l'établissement dans le cas notamment où l'utilisateur bénéficierait d'un accès à distance.

A cet égard, l'utilisateur s'engage à :

- à respecter les consignes relatives à la mise en œuvre de la connexion ;
- à ne pas pré enregistrer des procédures de connexion comportant l'identifiant et le mot de passe de l'utilisateur (ne pas cocher les cases de mémorisation de mot de passe).

En toute hypothèse, l'utilisateur, qui est responsable des équipements mis à sa disposition, en assure la garde. Il assiste l'établissement ou procède lui-même, selon les cas, à toutes les démarches (déclaration d'assurance, plainte etc.) rendues nécessaires à la suite d'un incident de quelque nature que ce soit. Il en informe immédiatement l'autorité hiérarchique dont il dépend.

L'utilisation des équipements informatiques nomades impose un niveau de surveillance et de confidentialité renforcé.

L'utilisation de disquettes, CD-Rom et DVD doit respecter, en toute hypothèse, les règles édictées pour éviter tout risque de contamination par les virus.

L'utilisation d'équipements nomades exige, en l'absence de synchronisation automatique entre les équipements nomades et fixes, que l'utilisateur qui en fait usage veille à procéder aux sauvegardes nécessaires sur son poste de travail fixe.

7.5 Téléphonie

Chaque utilisateur dans le cadre de son activité professionnelle peut disposer, selon son profil, de moyens de télécommunication permettant l'échange de données et le transfert de la voix.

Ces outils de télécommunication consistent en des équipements terminaux de télécommunication (poste téléphonique fixe ou poste téléphonique mobile) ou de terminaux d'ordinateur permettant de bénéficier d'une téléphonie sous IP.

Par ailleurs, dans le cadre de la réalisation de ses activités, l'établissement utilise les services d'un réseau privé virtuel réservé à l'usage interne de l'ensemble des utilisateurs.

Il appartient à chaque utilisateur de respecter les conditions d'utilisation et d'échange de messages téléphoniques par transfert de données et transfert de la voie sur l'ensemble des outils de télécommunication mis à sa disposition.

En particulier, chaque utilisateur doit veiller au respect des règles portées à sa connaissance et relatives à l'utilisation du réseau privé virtuel de l'établissement.

L'attention de l'utilisateur est attirée sur le fait que l'accès à certains numéros peut être interdit et que des mesures techniques peuvent être mises en œuvre pour empêcher un tel accès.

Pour l'utilisation de l'ensemble de ces outils de télécommunications, chaque utilisateur se doit de prendre en considération et respecter les dispositions de la présente charte.

Il est expressément interdit à l'utilisateur d'utiliser la téléphonie mobile à des fins personnelles.
En aucune manière, l'utilisateur n'est autorisé à utiliser la téléphonie mobile pour prendre des photographies présentant un caractère non professionnel.

7.6 Messagerie électronique

7.6.1 Emission et réception des messages électroniques

L'utilisation de la messagerie électronique à des fins personnelles est admise. Elle ne doit pas nuire à la qualité du travail, ni au temps consacré à ce dernier. En cas d'abus de la part de l'utilisateur, l'autorité hiérarchique dont il dépend se réserve la faculté de supprimer cette tolérance.

Une adresse électronique nominative professionnelle est attribuée à l'utilisateur.

Les messages électroniques envoyés et reçus par l'utilisateur sont automatiquement archivés, à l'exception de ceux portant la mention « PRIVE » ou « Privé ».

L'utilisateur doit s'assurer attentivement de l'identité et de l'exactitude des adresses des destinataires des messages.

L'utilisateur doit en outre veiller à ce que la diffusion soit limitée au destinataire concerné afin d'éviter la diffusion de messages en masse, ce qui pourrait encombrer la messagerie, engendrer des temps de réponse longs et porter ainsi atteinte au bon fonctionnement du système d'information de l'établissement.

L'utilisateur peut constituer un annuaire pour faciliter l'envoi des messages, sous réserve du respect des règles établies dans la présente charte relatives, notamment, à la confidentialité des informations.

Tous les messages émis et reçus sont classés dans un chrono électronique ou papier.

L'émission ou la réception des messages électroniques peut être effectuée à partir ou à destination de la boîte de service lorsque le contenu du message nécessite une telle utilisation.

Les listes de diffusion internes sont autorisées dans la mesure où elles visent un nombre restreint de destinataires et que le message a un caractère professionnel.

Les listes de diffusion externes, c'est-à-dire à l'attention de destinataires ne faisant pas partie du périmètre de l'établissement, sont autorisées.

D'une manière générale, les listes de diffusion générales sont autorisées sur accord exprès de la direction.

7.6.2 Contenu des messages électroniques

Un message électronique permet d'échanger des informations à vocation professionnelle et liées à l'activité directe de l'établissement.

Il appartient à l'utilisateur d'adopter un comportement loyal et digne dans le cadre de l'utilisation de la messagerie électronique. Tout message à caractère injurieux, insultant, dénigrant, diffamatoire, dégradant, politique est interdit. En toute hypothèse, l'utilisateur s'engage à ne pas porter atteinte aux droits des tiers et à l'image et à la réputation de l'établissement.

Un message électronique peut contenir des textes, des images fixes ou animées à l'exclusion des films et des vidéos. En revanche, sauf autorisation expresse de l'administrateur, il ne peut pas contenir de sons et musiques (les casques ne sont pas autorisés).

Un message électronique peut contenir des télécopies. Toutes les règles établies par la présente charte s'appliquent à un tel document dès lors qu'il est transmis par la messagerie

La direction des systèmes d'information se réserve la faculté d'isoler, de façon temporaire, tout message douteux (porteur d'un virus, accompagné d'une pièce jointe litigieuse ou d'une pièce jointe trop volumineuse, etc.) et de le supprimer, le cas échéant. L'utilisateur est informé du traitement ainsi effectué du message douteux, en fonction des caractéristiques des filtres anti-spam utilisés.

L'attention des utilisateurs est attirée sur le fait que les messages électroniques échangés avec des tiers peuvent, sur le plan juridique et dans certains cas, former un contrat. Par ailleurs, l'utilisateur autorisé doit avoir conscience que tout engagement pris au nom de l'établissement peut constituer une preuve ou un commencement de preuve. Dans ces conditions, l'utilisateur doit être vigilant sur la nature des messages électroniques qu'il échange.

7.6.3 Signature des messages électroniques

Cette signature fait l'objet d'une forme standardisée.

Chaque utilisateur s'engage à respecter cette forme en évitant tout élément complémentaire.

7.6.4 Pieds des messages électroniques

Toutes les communications électroniques envisagées par les utilisateurs doivent insérer la formule de confidentialité et de réserves définie par l'établissement.

7.6.5 Consultation de la messagerie électronique

Chaque utilisateur doit consulter sa messagerie électronique au moins une fois par jour de présence.

Au cas où un utilisateur ne respecterait pas cette fréquence, il pourrait être tenu responsable des conséquences qui pourraient résulter d'un éventuel retard dans le traitement des messages.
En cas d'absence, l'utilisateur devra activer la fonction d'agent d'absence afin d'avertir son correspondant de son absence et limiter ainsi l'envoi des messages pendant son absence.

En raison de caractère professionnel de la messagerie électronique, il est important de s'assurer la continuité du traitement des messages et pour cela, les absences pour cause de congés ou maladie sont gérées de la façon suivante :

Quel que soit le cas, il est mis en place un indicateur d'absence qui signale l'absence d'ouverture du message dans les premières heures suivant sa réception.

En cas de maladie, si l'utilisateur n'a pas désigné de délégué de principe au moment de l'ouverture de sa boîte, le message est automatiquement rerouté vers une boîte imposée.

Le délégué s'engage à utiliser les informations en application des règles en vigueur dans l'établissement.

Il ne peut pas y avoir de reroutage vers des boîtes extérieures au système d'information de l'établissement.

7.6.6 Stockage des messages électroniques

L'utilisateur s'engage à faire régulièrement l'inventaire des messages les plus anciens et de détruire les messages qui ne présentent plus d'intérêt.

Il est également demandé d'éviter le double stockage des pièces jointes (dans le message et dans un fichier indépendant).

Tous les messages reçus et émis doivent être classés par l'utilisateur soit sur le disque dur, soit sur le serveur mis à disposition par le SDIS 04. Tout stockage de messages sur un disque dur ou un serveur qui ne serait pas mis à disposition de l'utilisateur par l'établissement est formellement interdit.

A cet égard, l'utilisateur pourra déterminer avec son supérieur hiérarchique la nature probante d'un message et l'utilité de sa sauvegarde.

7.6.7 Messages privés / répertoires privés

Tout message électronique à caractère privé émis ou reçu doit comporter, dans son objet, la mention « PRIVE » ou « privé ». Tout message ne comportant cette mention est réputé être un message professionnel, susceptible d'être consulté par tout utilisateur, habilité à le faire, et par l'autorité hiérarchique dont il dépend et ce, pour les besoins de l'établissement.

Tout message électronique portant par erreur la mention « PRIVE » ou « privé » doit être immédiatement réaffecté, afin qu'il puisse être convenablement archivé.

Il appartient à l'utilisateur de procéder au stockage de ses messages personnels dans un répertoire intitulé « PRIVE » ou « privé », répertoire qui doit être crée dans le disque dur de son ordinateur ou sur le réseau. En toute hypothèse, ce répertoire ne fait l'objet d'aucune mesure de sauvegarde et/ou de restauration. La sauvegarde de ce répertoire incombe donc à l'utilisateur sous sa seule responsabilité.

Il appartient à l'utilisateur de s'assurer de la licéité du contenu de son répertoire. En toute hypothèse, l'utilisateur s'interdit de stocker des images et du son dans répertoire « PRIVE » ou « privé ».

Le répertoire « PRIVE » ou privé » doit être supprimé par l'utilisateur au plus tard la veille de son départ de l'établissement. A défaut de procédure judiciaire ou enquête administrative, ce répertoire est automatiquement supprimé le lendemain du départ de l'utilisateur, sans être consulté et sans qu'aucune copie ne soit réalisée.

7.7 Répertoire individuel professionnel non partage

Un répertoire individuel professionnel non partagé est mis à la disposition de chaque utilisateur sur le serveur.

Ce répertoire n'est pas accessible aux autres utilisateurs, sauf volonté contraire expresse manifestée par l'utilisateur. En revanche, le répertoire est accessible à l'autorité hiérarchique dont il dépend, qui procède à des sauvegardes régulières.

Ce répertoire est limité à 100 Mo et ne peut recevoir que les fichiers de la suite office et PDF.

7.8 Internet

L'accès à l'Internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par les administrateurs conformément à la politique de sécurité en vigueur.

L'utilisation de l'internet à des fins personnelles est admise. En cas d'abus de la part de l'utilisateur, l'autorité hiérarchique dont il dépend se réserve la faculté de supprimer cette tolérance.

En toute hypothèse, l'utilisateur s'interdit de procéder aux téléchargements de fichiers ou logiciels et notamment les logiciels de partage de données pouvant permettre un accès par des tiers au disque dur de l'établissement, sauf autorisation expresse de l'autorité hiérarchique dont il dépend. L'utilisateur peut se rapprocher du correspondant chartes en cas de doute.

L'utilisateur est informé que l'accès à certains sites est rendu impossible par la direction des systèmes d'information. L'utilisateur s'interdit de contourner les mesures techniques de blocage et de filtrage ou toutes mesures de protection mises en œuvre par la direction des systèmes d'information.

L'utilisateur est en outre informé que l'établissement a mis en place un système permettant d'assurer la traçabilité des accès internet et/ou des données échangées et se réserve le droit de procéder au filtrage des sites dont elle n'autorise pas l'accès, comme au contrôle a posteriori des sites ou des pages visitées et de la durée des accès correspondants, et ce dans le respect des dispositions légales applicables. Les traces correspondantes aux connexions et aux sites internet accédés par l'utilisateur sont conservées pendant une durée variable et feront l'objet d'une formalité préalable auprès de la Cnil.

Tout abonnement payant à un site devra faire l'objet d'une concertation préalable avec la direction (...) pour une meilleure gestion de ces abonnements.

L'utilisateur s'interdit de participer à toute forme de forum de discussion, de chat ou de messagerie instantanée hors contexte professionnel.

Il est demandé à chaque utilisateur de se conformer aux dispositions du guide de l'utilisateur pour déterminer ses droits dans le cadre de la consultation de sites internet, ainsi que les droits de l'établissement.

A cet égard, il est précisé à chaque utilisateur que la libre accessibilité aux informations contenues dans les sites internet auxquels il accède n'inclut pas la libre réutilisation desdites informations dans le cadre d'une activité professionnelle.

7.9 Réseaux sociaux

Par ailleurs, l'établissement estime que les réseaux sociaux extérieurs à l'établissement occupent une place grandissante. Ces réseaux permettent à ses agents de créer de nouvelles relations avec des partenaires et d'optimiser la communication autour des services.

Cependant, l'utilisation des réseaux sociaux peut être source de risques et de responsabilité notamment en termes d'image. Aussi, afin de limiter les risques encourus, les règles suivantes ont été arrêtées.

7.9.1 Usage professionnel

Dans le cadre de la sphère professionnelle, l'agent doit obtenir au préalable l'autorisation de son supérieur hiérarchique pour pouvoir participer à un réseau social et/ou créer un espace sur un réseau social.

Si l'autorisation a été donnée, l'agent doit se conformer aux règles et instructions édictées par son supérieur hiérarchique, ce dernier étant seul compétent pour déterminer les conditions d'utilisation du réseau social.

De plus, l'agent devra :

- s'abstenir de publier un contenu de façon anonyme et, au contraire, s'identifier clairement, en précisant sa fonction au sein de l'établissement ;
- répondre aux contributions des tiers avec pertinence, exactitude, en s'efforçant de promouvoir l'image de l'établissement ;
- respecter les conditions générales d'utilisation du réseau social et l'ensemble des lois applicables ;
- utiliser uniquement les outils de communication de l'établissement, selon les instructions qui lui ont été données ;
- s'abstenir de diffuser toute information confidentielle ou sensible relative à l'établissement ;

En cas de doute sur l'utilisation d'un réseau social, l'utilisateur devra consulter son supérieur hiérarchique.

L'autorisation donnée pourra être retirée, modifiée ou suspendue par le supérieur hiérarchique dès lors que l'intérêt de l'établissement le justifie.

L'agent devra prendre toutes les précautions utiles pour que son utilisation des réseaux sociaux soit sans danger pour le système d'information de l'établissement.

7.9.2 Usage personnel

Dans le cadre de l'utilisation personnelle des réseaux sociaux, l'agent s'interdit de communiquer la moindre information sur son activité professionnelle, en particulier des informations confidentielles, des informations sensibles relatives à l'établissement ou pouvant porter préjudice à ce dernier.

7.9.3 Signalement

Qu'il utilise les réseaux sociaux à titre professionnel ou non professionnel, l'agent s'engage à informer son supérieur hiérarchique de tout agissement de tiers susceptible de porter atteinte à la réputation de l'établissement ou à un droit de l'établissement (notamment de propriété intellectuelle) dont il aurait connaissance.

7.10 Intranet

L'intranet permet à l'utilisateur d'accéder à différentes fonctions et informations en relation avec l'établissement (annuaires, trombinoscopes, applications informatiques, etc.) et ce, en fonction du profil attribué.

L'accès à l'intranet est réservé à un usage exclusivement professionnel.

Cet accès peut être réalisé à distance via un VPN.

7.11 Travail à distance

L'utilisateur peut, sur autorisation de l'établissement se voir octroyer une autorisation d'accès à distance, via le serveur VPN de l'établissement, à l'intranet de l'établissement.

Cet accès est réalisé, selon le cas, par le biais des moyens de communications électroniques mis à la disposition de l'agent par l'établissement, ou par les moyens de communications électroniques appartenant à l'agent, sur autorisation de l'établissement.

Dans tous les cas, il est interdit à l'utilisateur d'user de ce droit d'accès au-delà de ses horaires ou heures légales de travail, en fonction de son statut.

La connexion à distance étant par définition sous le contrôle de l'utilisateur, celui-ci a la responsabilité du respect de cette interdiction.

7.12 Web – Plates-formes collaboratives - Forums de discussion

La mise en place ou la consultation ou la participation à certains services spécifiques sur l'Internet (tels que des espaces collaboratifs de stockage externe à l'établissement ou des blogs) ne peut se faire que sur autorisation écrite et préalable de l'autorité hiérarchique dont il dépend au regard des nécessités de l'activité professionnelle des utilisateurs concernés.

7.12.1 Plate-forme collaborative externe professionnelle

L'utilisateur sur autorisation écrite et préalable de l'autorité hiérarchique dont il dépend peut au regard des nécessités de son activité professionnelle participer à des plates-formes collaboratives externes professionnelles.

L'utilisateur accédant à une plate-forme collaborative externe professionnelle est informé qu'il agit au nom de l'établissement et qu'il doit donc en permanence veiller à ne pas porter atteinte aux intérêts de cette dernière, ni aux droits de tiers.

L'utilisateur doit être particulièrement vigilant à l'égard de la nature des informations, qu'il communique et s'en référer à son supérieur hiérarchique en cas de doute.

L'utilisateur doit s'assurer que chaque participant est tenu à une stricte confidentialité à l'égard des informations qu'il est amené à connaître dans le cadre de sa participation à la plate-forme collaborative externe professionnelle.

La participation à une plate-forme collaborative externe professionnelle doit toujours s'effectuer dans le cadre d'une totale transparence et à ce titre, les participants ne peuvent intervenir de façon anonyme ni utiliser de pseudonyme ou emprunter une quelconque identité fictive.

Les contributions respectives des participants sur les documents doivent être clairement identifiées et, à défaut, l'origine de chaque document et contribution doit être indiquée.

L'utilisateur doit dans ce cadre veiller à la traçabilité des interventions effectuées par chaque participant sur les documents élaborés, modifiés et échangés.

7.12.2 Forums de discussion

7.12.2.1 Forums externes

Les forums de discussion, les « News Group » ou les communautés auxquelles participent les utilisateurs ont une finalité exclusivement professionnelle et font l'objet d'une autorisation de l'autorité hiérarchique dont il dépend.

L'utilisateur se connectant à un forum de discussion professionnel doit veiller à ne pas porter atteinte aux intérêts de l'établissement au nom de laquelle il agit et des tiers.

La participation aux forums doit toujours s'effectuer dans le cadre d'une totale transparence et à ce titre, les participants ne peuvent intervenir de façon anonyme ni utiliser de pseudonyme ou emprunter une quelconque identité fictive.

7.12.2.2 Forums internes

L'ouverture d'un forum professionnel interne, de type « News Group » ou d'une communauté par un utilisateur s'effectue sur autorisation écrite de l'autorité hiérarchique dont il dépend.

Les forums créés au sein de l'établissement font l'objet d'un contrôle par un modérateur désigné comme étant responsable de l'animation du forum concerné.

Toutefois, une fois créé il n'entre pas dans les prérogatives du modérateur de clôturer définitivement un forum. Les forums ne font pas l'objet d'une procédure de clôture automatique.

Les utilisateurs sont informés que les messages circulant sur les forums autorisés ne sont pas nécessairement sauvegardés. Il appartient donc à chacun des utilisateurs de sauvegarder les messages qui lui sont utiles.

7.12.3 Gestion des connaissances et de l'espace collaboratif

Le SDIS 04 privilégie le partage et la capitalisation des connaissances, et peut être ainsi amené à mettre en place des espaces collaboratifs de travail.

La qualité des informations ainsi disponibles est un objectif élevé et chaque utilisateur s'engage à :

- contribuer à la gestion des connaissances mise en place ;
- être attentif à la pertinence des informations diffusées au sein de ces espaces et à travers les outils de gestion des connaissances mis à sa disposition par le SDIS 04.

Par souci de qualité, de responsabilité et de protection du patrimoine informationnel du SDIS 04, l'utilisation de ces mêmes espaces et outils peut faire objet d'opérations de contrôle, d'audit, de modération et de traçabilité renforcées. Les utilisateurs seront avertis de la présence de tels outils.

7.12.4 Messagerie instantanée

Il est interdit à l'utilisateur d'utiliser d'autres systèmes de messagerie instantanée que ceux mis à sa disposition par le SDIS 04.

8 Données à caractère personnel

8.1 Utilisateurs des données

Les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitement automatisé ou manuel de données à caractère personnel.

Aucun traitement de données à caractère personnel ne peut être mis en œuvre par l'utilisateur sans accord préalable de l'autorité hiérarchique dont il dépend et réalisation des formalités préalables nécessaires auprès de la Cnil sauf exception légale. L'utilisateur devra ainsi tout particulièrement veiller à ne pas transférer des données vers l'étranger (pays hors Union européenne) sans autorisation de l'autorité hiérarchique dont il dépend.

8.2 Droits des personnes

Les données concernant les utilisateurs sont collectées et traitées de manière loyale et licite par l'établissement au titre de sa mission de gestion des ressources informatiques.

Les traitements opérés dans le cadre de la présente charte ont pour finalités :

- le suivi et la maintenance des ressources informatiques ;
- la définition des autorisations d'accès aux applications et réseaux ;
- la mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement du système d'information ;
- la sécurité des ressources informatiques et système d'information ;
- la gestion de la messagerie électronique professionnelle ;
- la gestion administrative de l'établissement ;
- le respect de la présente charte.

Conformément à la loi « Informatique et libertés », les utilisateurs sont informés qu'ils disposent d'un droit d'accès, de rectification, et d'opposition pour motif légitime, relatif à l'ensemble des informations à caractère personnel les concernant. Ce droit s'exerce auprès du service désigné à cet effet par le SDIS 04.

9 Loi en vigueur et réglementation

Les utilisateurs sont informés que l'ensemble des règles légales et réglementaires s'applique dans le cadre de l'utilisation des ressources informatiques.

Il en est ainsi sans que cette liste soit exhaustive :

- du droit d'auteur qu'il s'agisse de créations multimédia, de logiciels, de textes, de photos, d'images de toute nature, étant souligné que toute mention relative aux droits de l'auteur ne peut faire l'objet d'une suppression et que toute reproduction, adaptation ou modification de l'œuvre de celui-ci sans son consentement constitue une contrefaçon susceptible de sanctions pénales ;
- des dispositions relatives à la fraude informatique, qu'il s'agisse de l'intrusion dans un système de traitement automatisé de données ou de l'altération des éléments qu'il contient ;
- des règles d'ordre public, les informations portant atteinte à l'intégrité ou à la sensibilité des autres utilisateurs par accès à des messages, images ou textes provoquant ou incitant à la haine ;des règles en matière de traitement automatisés ou manuels de données à caractère personnel ;
- la présente charte est complétée par le « guide de l'utilisateur » précisant les principales dispositions légales et réglementaires en vigueur, qui s'imposent à tous les utilisateurs.

10 Mesures de contrôle

10.1 Surveillance

10.1.1 Direction des systèmes d'information

Les ressources informatiques peuvent donner lieu à surveillance et contrôle à des fins statistiques de traçabilité, d'optimisation, de sécurité ou de détection des abus.

La direction des systèmes d'information peut diligenter toutes opérations techniques de contrôle permettant de vérifier le respect des dispositions de la présente charte ou des règles légales.

Dans le cadre de ces opérations de contrôle nécessaire au bon fonctionnement du système d'information, l'utilisateur est informé que les personnes mandatées par la direction des systèmes d'information peuvent notamment être amenées à ouvrir tout

message ou fichier figurant sur sa messagerie et/ou dans son répertoire nommé « PRIVE » ou « privé », et à vérifier l'ensemble des connexions dudit utilisateur.

Lors de ces accès, ces personnes sont tenues de respecter la confidentialité des informations, auxquelles elles accèdent, vis-à-vis des tiers à la mission de surveillance et de contrôle.

L'usage des services Internet peut faire l'objet d'un contrôle a posteriori. Ce contrôle peut porter sur le temps de connexion par poste ou sur les sites les plus consultés.

10.1.2 Autorité hiérarchique

L'autorité hiérarchique s'engage à réaliser les contrôles qu'elle estime indispensable à la sauvegarde des intérêts de l'établissement, dans le respect strict des dispositions légales et réglementaire en vigueur.

10.2 Maintenance

La mise à disposition de ressources informatiques implique nécessairement des opérations de maintenance technique, qu'il s'agisse de maintenance corrective, de maintenance préventive ou de maintenance évolutive.

Ces opérations de maintenance peuvent nécessiter l'intervention d'une personne habilitée sur site ou sous la forme d'une prise de main à distance (télémaintenance). La personne habilitée est la personne désignée à cet effet par l'établissement.

L'utilisateur sera informé de cette prise de main à distance par un message d'information apparaissant sur son écran. Sans la validation du message d'information par l'utilisateur, la personne habilitée en charge de la maintenance ne pourra intervenir.

L'objectif de ces opérations n'est autre que d'assurer le bon fonctionnement et la sécurité des systèmes d'informations. Cependant dans le cadre de ces interventions, la « personne habilitée » peut être amenée à prendre connaissance de messages émis ou reçus par l'utilisateur et à examiner en détail le journal de ses connexions.

La personne habilitée fera en sorte de ne pas accéder au fichier intitulé « PRIVE » ou « Privé » en dehors de la présence de l'utilisateur. Cependant, elle peut y être contrainte pour des raisons de sécurité ou pour des raisons techniques (surcharge du système, lutte anti-virus, lutte anti-spam, etc.) et ce, malgré l'opposition de l'utilisateur. La personne habilitée est tenue en tout état de cause à une stricte obligation de confidentialité à l'égard des informations qu'elle peut être amenée à connaître dans le cadre de ses activités.

11 Accès par des tiers aux ressources informatiques

Les utilisateurs prestataires tiers ayant accès aux ressources informatiques sont soumis aux dispositions de la « charte des tiers » qui doit avoir été communiquée et avoir été acceptée par l'employeur.

Pour toutes questions concernant la procédure devant être scrupuleusement respectée avant de permettre à une personne intervenante extérieure d'accéder aux ressources informatiques, vous pouvez interroger le correspondant chartes.

En cas de violation, par un tiers, des procédures applicables, l'établissement se réserve le droit soit :

- de demander à l'employeur de la personne intervenante son remplacement sans délai, par une personne intervenante de niveau et de compétences équivalentes ;
- de rompre le lien contractuel qui la lie à l'employeur de la personne intervenante.

12 Entrée en vigueur

La présente charte a fait l'objet d'une consultation par le comité technique, lequel a donné un avis favorable.

La présente charte entre en vigueur à compter du [A COMPLETER].

Chaque utilisateur, destinataire de la présente charte, est invité à transmettre à la direction toute proposition de modification ou d'ajout, dont il a pu constater l'intérêt dans le cadre de sa pratique professionnelle.

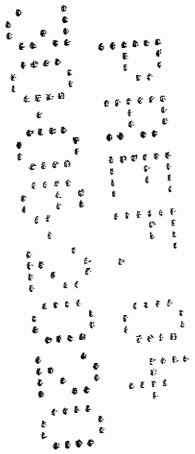
La présente charte sera régulièrement mise à jour par la direction et pourra faire l'objet d'adaptations spécifiques en fonction des catégories d'utilisateurs concernés.

sdis sapeurs pompiers
Alpes de Haute-Provence

GUIDE UTILISATEUR
RELATIF AUX AGENTS PUBLICS

MARS 2020 > V 3.0

SOMMAIRE



1 Préambule

Le présent guide s'inscrit dans le cadre de la politique de sécurité mise en place par le SDIS 04

Il a pour objet d'exposer aux utilisateurs les principales dispositions légales et réglementaires qui s'appliquent dans le cadre de l'utilisation des ressources informatiques et que les utilisateurs s'engagent à respecter.

L'énumération des règles exposées au présent guide n'est pas exhaustive.

L'utilisateur s'engage, par ailleurs, à se tenir informé de l'évolution de ces règles et de toute nouvelle règle pouvant s'appliquer.

2 Les règles en matière de protection des biens incorporels

2.1 Les créations intellectuelles

2.1.1 Dispositions générales

En vertu des règles du Code de la propriété intellectuelle, l'auteur d'une œuvre de l'esprit jouit, sur cette œuvre, du seul fait de sa création, « d'un droit de propriété incorporel et exclusif opposable à tous »[1].

Cette disposition s'applique à toutes les œuvres de l'esprit, quel qu'en soit le genre, la forme d'expression, le mérite ou la destination. Sont considérées ainsi comme des œuvres de l'esprit, au sens du Code de la propriété intellectuelle, les œuvres suivantes:

- « les livres, brochures et autres écrits littéraires, artistiques et scientifiques ;
- les conférences, allocutions, serments, plaidoiries et autres œuvres de même nature ;
- les œuvres dramatiques et dramatique-musicales ;
- les œuvres chorégraphiques ;
- les œuvres musicales avec ou sans paroles ;
- les œuvres cinématographiques et autres œuvres consistant dans des séquences animées d'images sonorisées ou non, dénommées ensemble œuvres audiovisuelles ;
- les œuvres de dessin, de peinture, d'architecture, de sculpture, de gravure, de lithographie ;
- les œuvres graphiques et typographiques ;
- les œuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie ;
- les œuvres d'art appliqué ;
- les illustrations, les cartes géographiques ;
- les plans, croquis et ouvrages plastiques relatifs à la géographie, à la topographie, à l'architecture et aux sciences ;
- les logiciels, y compris le matériel de conception préparatoire »[2].

Toute forme d'utilisation, de reproduction, de représentation ou de mise à disposition du public de l'œuvre est ainsi soumise à l'autorisation préalable du titulaire des droits sur les œuvres.

[1] CPI. art. L.111-1.
[2] CPI. art. L.112-2.

L'utilisateur est donc informé qu'à défaut d'une autorisation expresse du titulaire, il lui est interdit d'utiliser, reproduire, représenter ou mettre à disposition du public une œuvre.

L'utilisateur ne doit pas utiliser l'accès internet mis à sa disposition par le SDIS 04 pour reproduire ou représenter des œuvres de l'esprit sans l'autorisation des titulaires des droits[3].

La contrefaçon d'une œuvre de l'esprit est punie de trois ans d'emprisonnement et 300 000 euros d'amende[4].

1.1.2 Les logiciels

Les logiciels sont protégés par le droit d'auteur.

Toute utilisation, reproduction, représentation ou mise à disposition du public du logiciel n'est autorisée que sous réserve de l'autorisation expresse du titulaire des droits sur ledit logiciel.

L'étendue et les caractéristiques des droits conférés sont définies par des contrats de licence d'utilisation qui précisent les modalités selon lesquelles est autorisée l'utilisation du logiciel visé.

L'utilisateur d'un logiciel s'expose à des sanctions civiles et pénales prévues par le Code de la propriété intellectuelle, lorsqu'il utilise le logiciel sans autorisation (ou au-delà des limites visées dans les contrats de licence).

Par ailleurs, les utilisateurs sont informés que de tels actes exposent également le SDIS 04 à des risques importants, notamment en termes de sécurité informatique.

A ce titre, les utilisateurs doivent notamment :

- utiliser les logiciels mis à leur disposition dans le cadre de leurs missions, dans le respect des droits et obligations prévues par les licences d'utilisation souscrites par SDIS 04 ;
- ne pas reproduire ou diffuser les logiciels mis ainsi à leur disposition.

L'utilisateur ne peut, par exemple, enregistrer ou télécharger un programme auquel il a eu accès dans le cadre de ses fonctions au sein du SDIS 04, afin de l'enregistrer sur son propre poste pour toute autre utilisation hors du cadre de ses fonctions et/ou hors des locaux du SDIS 04.

De la même manière, l'utilisateur ne peut installer ou télécharger sur des équipements du SDIS 04 des logiciels sur lesquels des droits lui auraient été concédés à titre personnel (contrat de licence souscrit par lui-même pour ses besoins personnels) et dont l'utilisation à des fins professionnelles au sein du SDIS

[3] L'article L.335-7 du code de la propriété intellectuelle modifiée par l'article 8 de la loi du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet dite Hadopi 2 énonce que : « Pour les contraventions de la cinquième classe prévues par le présent code, lorsque le règlement le prévoit, la peine complémentaire définie à l'article L. 335-7 peut être prononcée selon les mêmes modalités, en cas de négligence caractérisée, à l'encontre du titulaire de l'accès à un service de communication au public en ligne auquel la commission de protection des droits, en application de l'article L. 331-25, a préalablement adressé, par voie d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation, une recommandation l'invitant à mettre en œuvre un moyen de sécurisation de son accès à internet ». Il convient donc de rappeler aux utilisateurs qu'ils doivent veiller à la protection des droits de propriété intellectuelle des tiers. En outre, la société doit mettre en place des moyens de sécurisation offerts par le fournisseur d'accès pour veiller à ce que l'accès internet ne soit pas utilisé pour reproduire ou représenter des œuvres sans autorisation de l'auteur.

[4] CPI. art. L.335-2.

04 ne rentrerait pas dans le cadre de l'étendue des droits conférés sur l'œuvre en question.

L'utilisateur est en outre informé que :

- les logiciels « shareware » sont en libre essai, mais non libres de droits ;
- la licence « GPL », est une licence comme une autre qui contient droits et obligations à la charge de l'auteur et de l'utilisateur. Plus généralement, « logiciel libre » ne signifie pas logiciel sans droits.

1.1.3 Les textes, images et sons

De la même façon, les textes, les images et les sons, sont, dès lors qu'ils présentent une certaine originalité, protégés par le droit d'auteur.

L'autorisation expresse du titulaire des droits est nécessaire pour leur utilisation, reproduction, représentation et mise à disposition du public.

Le non-respect des droits de l'auteur sur ces éléments est constitutif de contrefaçon et est donc civilement et/ou pénalement sanctionnable[5].

D'une manière générale, la difficulté à connaître précisément l'origine de tels éléments transmis et, donc, les droits y afférents, en particulier avec le développement des moyens d'échange d'informations en réseau ouvert comme Internet, oblige les utilisateurs à la plus grande prudence.

Les utilisateurs doivent donc s'interdire d'utiliser les éléments sur lesquels ils ne disposeraient pas d'autorisation expresse d'utilisation.

S'agissant des éléments mis à leur disposition dans le cadre de leurs missions, les utilisateurs s'engagent à ne les utiliser qu'à des fins strictement professionnelles.

1.1.4 Les bases de données

On entend par base de données un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen.

Les bases de données qui, par le choix ou les dispositions des matières, constituent des créations intellectuelles, sont soumises aux dispositions du Code de la propriété intellectuelle.

Par ailleurs, les données contenues dans ces bases sont protégées par le droit sui generis du producteur de base de données lequel fait obstacle :

- à toute extraction par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ;
- à la réutilisation, par la mise à disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle que soit sa forme[6].

[5] CPI. art. L.335-2.
[6] CPI. art. L.342-1.

1.1.5 Négligence caractérisée

L'utilisateur est tenu de se conformer à la politique de sécurité du SDIS 04, y compris aux règles d'utilisation des moyens de sécurisation mis en œuvre dans le but de prévenir l'utilisation illicite des ressources, et de s'abstenir de tout acte portant atteinte à l'efficacité de ces moyens.

Le titulaire d'un accès à Internet et donc le SDIS 04 est tenu de sécuriser cet accès afin qu'il ne soit pas utilisé 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. S'il ne se conforme pas à cette obligation, le titulaire peut voir sa responsabilité pénale engagée au titre de la négligence caractérisée[7]. Cette contravention est punie d'une peine d'amende d'un montant maximum de 1500 euros pour les personnes physiques et 7500 euros pour les personnes morales, qui peut être assortie d'une peine de suspension de l'accès à internet d'une durée maximum d'un mois. Ces sanctions sont prononcées par le juge judiciaire.

Cette responsabilité du titulaire de l'accès n'exclut en rien celle de l'utilisateur qui peut se voir reprocher un délit de contrefaçon[8].

2.2 Les signes distinctifs

Le Code de la propriété intellectuelle protège toute marque de fabrique, de commerce ou de service servant à distinguer les produits ou services d'une personne physique ou morale[9].

Peuvent être utilisés à titre de marque, toutes les dénominations et signes figuratifs ou sonores, tels que les mots, assemblages de mots, noms patronymiques, noms géographiques, pseudonymes, lettres, chiffres, sigles, emblèmes, photographies, dessins, empreintes, logos ou la combinaison de certains d'entre eux.

L'enregistrement de la marque confère à son titulaire un droit de propriété sur la marque pour les produits et services qu'il a désignés.

L'utilisateur ne peut, sauf autorisation du propriétaire, reproduire, utiliser ou apposer une marque pour des produits et services identiques à ceux désignés dans l'enregistrement, ou encore supprimer ou modifier une marque régulièrement apposée.

L'utilisateur ne peut, par ailleurs, sauf autorisation du propriétaire, s'il existe un risque de confusion dans l'esprit du public :

- reproduire, utiliser ou apposer une marque pour des produits ou services similaires à ceux désignés dans l'enregistrement ;
- limiter une marque et l'utiliser, pour des produits ou services identiques ou similaires à ceux désignés lors de l'enregistrement.

Dans ces conditions, l'utilisateur ne saurait notamment, dans le cadre de ses fonctions, utiliser une marque pour laquelle le SDIS 04 ne détient pas l'autorisation expresse d'utilisation.

Il ne saurait, en outre, utiliser à des fins personnelles, toute marque dont le SDIS 04 serait titulaire.

[7] CPI. art. L.335-7-1.
[8] CPI. art. L.335-3.
[9] CPI. art. L.711-1.

2.3 Les inventions et autres créations

Certains éléments faisant partie du patrimoine du SDIS 04 sont susceptibles d'être protégés par :

- le droit des dessins et modèles ;
- ou le droit des brevets.

Par conséquent, l'utilisateur s'interdit de les utiliser sans l'autorisation expresse de l'autorité hiérarchique.

2.4 Les dénominations non protégées par un droit de propriété intellectuelle

A noter que certaines dénominations du SDIS 04, qui ne sont pas protégées par un droit de propriété intellectuelle, bénéficient d'une protection et ne peuvent, par conséquent, être utilisées sans autorisation :

- une dénomination sociale ou raison sociale ;
- un nom de domaine.

Par conséquent, l'utilisateur s'interdit de les utiliser sans l'autorisation expresse de l'autorité hiérarchique.

3 Les règles en matière de protection des systèmes de traitement automatisé de données (STAD)

3.1 L'accès ou le maintien dans un STAD

La notion d'accès s'entend de tout système de pénétration tels que la connexion pirate tant physique que logique, l'appel d'un programme alors que l'on ne dispose pas d'habilitation, l'interrogation d'un fichier sans autorisation.

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende (article 323-1 du Code pénal).

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende (article 323-1 du Code pénal).

Le maintien frauduleux est caractérisé par des états de situation anormale tels que connexion, visualisation ou opérations multiples, alors que l'accédant a pris conscience que ce maintien est « anormal ».

3.2 L'entrave au fonctionnement d'un STAD

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende (article 323-2 du Code pénal).

L'entrave au système est appréhendée de manière extrêmement large car il suffit d'une influence « négative » sur le fonctionnement du système pour que le concept d'entrave soit retenu.

Il en est ainsi pour les bombes logiques, l'occupation de capacité mémoire, la mise en place de codification, de barrage, ou tout autre élément retardant un accès normal.

3.3 Détention de programmes informatique portant atteinte à un STAD

L'utilisateur est informé qu'il est interdit de détenir, offrir, céder ou mettre à disposition, un équipement, un programme informatique sauf autorisation préalable du SDIS 04 et en raison de motifs légitimes[10] :

- permettant d'accéder ou de se maintenir frauduleusement dans un système de traitement automatisé ;
- permettant d'entraver ou de fausser le fonctionnement du système de traitement automatisé ;
- permettant d'introduire frauduleusement des données dans un système de traitement automatisé.

Le SDIS 04 doit donc veiller à ce que les utilisateurs ne détiennent pas de logiciels, équipements informatiques permettant par exemple d'accéder ou de se maintenir frauduleusement dans un système, ou permettant d'entraver ou de fausser le fonctionnement du système ou d'introduire frauduleusement des données sans un système.

3.4 L'introduction, la suppression ou la modification de données contenues dans un STAD

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende (article 323-3 du Code pénal).

4 Les règles en matière de protection des personnes

4.1 L'atteinte à la vie privée des personnes

Chacun a droit au respect de l'intimité de sa vie privée.

Ainsi, la diffusion de toute information qui relève de la sphère privée d'une personne est susceptible d'engager la responsabilité civile de l'auteur de cette diffusion[11].

Par information qui relève de la sphère privée des personnes, il faut entendre : des informations portant sur la vie sentimentale d'une personne, sur ses mœurs sexuelles, sur sa famille ou encore sur sa rémunération.

Par ailleurs, constitue une infraction, le fait, au moyen d'un procédé quelconque, de volontairement porter atteinte à l'intimité de la vie privée d'autrui :

en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé[12].

---

[10] Le code pénal réprime les atteintes aux systèmes de traitements automatisés de données (articles 323-1 et suivants du code pénal). En particulier l'article L.323-3-1 énonce que : « Le fait sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévus par les articles 323-1 et suivants du code pénal est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée».

[11] Cciv. art. 9.
[12] CP. art. 226-1.

Est également puni le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes visés ci-dessus.

4.2 Usurpation d'identité en ligne

Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération [sur un réseau de communication au public en ligne] est puni d'un an d'emprisonnement et de 15 000 euros d'amende[13].

4.3 L'utilisation des moyens informatiques à des fins privées

L'utilisation à des fins privées des ressources informatiques est tolérée par la jurisprudence sous réserve qu'elle demeure résiduelle[14].

Cette utilisation privative résiduelle ne doit pas nuire à l'exécution de la prestation de travail au temps consacré au travail ni au bon fonctionnement du système d'information du SDIS 04.

La mention « PRIVE » ou « Privé » dans l'objet des messages électroniques et/ou la dénomination des répertoires utilisés pour le stockage des messages et données à caractère privé permet d'attirer l'attention du SDIS 04. A défaut, les messages électroniques et données stockées dans le système d'information du SDIS 04 sont présumés professionnels.

4.4 L'atteinte aux droits de la personnalité

Il est strictement interdit d'utiliser le nom, l'image ou encore la voix d'une personne sans son autorisation.

Un tel acte est susceptible d'engager la responsabilité civile de son auteur.

4.5 L'atteinte à la représentation des personnes

Constitue une infraction le fait de publier, par quelque moyen que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention.

4.6 La dénonciation calomnieuse

L'attention de l'utilisateur est attirée sur le fait que la dénonciation, effectuée par tout moyen et dirigée contre une personne déterminée, d'un fait qui est de nature à entraîner des sanctions judiciaires, administratives ou disciplinaires et que l'on sait totalement ou partiellement inexact, lorsqu'elle est adressée :

soit à un officier de justice ou de police administrative ou judiciaire ;
soit à une autorité ayant le pouvoir d'y donner suite ou de saisir l'autorité compétente ;
soit aux supérieurs hiérarchiques ou à l'employeur de la personne dénoncée,

est punie de cinq ans d'emprisonnement et de 45 000 euros d'amende[15].

[13] CP art.226-4-1.
[14] Cass. soc. 2-10-2001 n° 99-42942.
[15] CP. art. 226-10.

La fausseté du fait dénoncé résulte nécessairement de la décision, devenue définitive, d'acquittement, de relaxe ou de non-lieu déclarant que la réalité du fait n'est pas établie ou que celui-ci n'est pas imputable à la personne dénoncée.

4.7 L'atteinte au secret professionnel

L'utilisateur doit avoir conscience que la révélation d'une information à caractère secret dont il est dépositaire, soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende[16].

4.8 L'atteinte au secret des correspondances électroniques

Constitue une infraction le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende[17].

Est également puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.

L'attention de l'utilisateur est ainsi attirée sur le fait qu'il doit s'interdire de prendre connaissance des courriers postaux ou électroniques qui ne lui sont pas adressés, à l'exception de ceux présentant un caractère professionnel et sous réserve qu'il soit habilité à le faire par l'autorité hiérarchique.

4.9 Les délits de presse

4.9.1 La diffamation publique

Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation[18].

La publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable, même si elle est faite sous forme dubitative ou si elle vise une personne ou un corps non expressément nommés, mais dont l'identification est rendue possible par les termes des discours, cris, menaces, écrits ou imprimés, placards ou affiches incriminés.

La diffamation commise envers les particuliers est punie d'une amende de 12 000 euros[19].

La diffamation commise envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée est punie d'un an d'emprisonnement et de 45 000 euros d'amende ou de l'une de ces deux peines seulement[20].

[16] CP. art. 226-13.
[17] CP. art. 226-15.
[18] L. 29 juillet 1881, art. 29.
[19] L. 29 juillet 1881, art. 32, al.1er.
[20] L. 29 juillet 1881, art. 32, al. 2.

Sera punie des peines prévues à l'alinéa précédent la diffamation commise envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap[21].

4.9.2 L'injure publique

Toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait est une injure[22].

L'injure commise envers les particuliers, lorsqu'elle n'aura pas été précédée de provocations, est punie d'une amende de 12 000 euros[23].

Sera punie de six mois d'emprisonnement et de 22 500 euros d'amende l'injure commise envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée[24].

Sera punie des peines prévues à l'alinéa précédent l'injure commise envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap[25].

4.10 La mise en péril des mineurs

Les ressources informatiques mises à la disposition des utilisateurs permettent l'accès à une communication et à une information importante et mutualisée.

Or, de telles ressources ne doivent pas permettre de véhiculer n'importe quelle information ou donnée.

Ainsi, est sanctionné pénalement le fait de consulter, de fixer, d'enregistrer ou de transmettre en vue de sa diffusion l'image d'un mineur lorsque cette dernière présente un caractère pornographique et de diffuser une telle image, par quelque moyen que ce soit[26].

Est également puni le fait de fabriquer, de transporter, de diffuser, par quelque moyen que ce soit et quel que soit le support, un message à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, lorsque ce message est susceptible d'être vu ou perçu par un mineur.

En conséquence, les ressources informatiques mises à la disposition des utilisateurs doivent être utilisées également dans le respect de ces règles.

5 LES REGLES EN MATIERE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, crée un dispositif juridique, pour encadrer la collecte et le traitement de données à caractère personnel.

[21] L. 29 juillet 1881, art. 32, al. 3.
[22] L. 29 juillet 1881, art. 29.
[23] L. 29 juillet 1881, art. 33 al. 1er..
[24] L. 29 juillet 1881, art. 33 al.3.
[25] L. 29 juillet 1881, art. 33, al. 4.
[26] CP. art. 227-23.

Une donnée à caractère personnel est définie comme toute information qui permet, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent.

Un traitement de données à caractère personnel, est défini comme toute opération ou tout ensemble d'opérations portant sur des données à caractère personnel, par exemple, sur le nom, le prénom, l'adresse postale ou le numéro d'immatriculation d'une personne, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

5.1 Les droits de la personne concernée par le traitement

La personne concernée par le traitement de données à caractère personnel est la personne physique à laquelle se rapportent les données qui font l'objet du traitement.

Cette personne bénéficie :

- d'un droit d'opposition qui lui permet de s'opposer, pour des motifs légitimes, à ce que ses données fassent l'objet d'un traitement ;
- d'un droit d'accès, qui lui permet d'obtenir des informations relatives aux données à caractère personnel traitées ;
- d'un droit de modification ou de suppression des données.

5.2 L'atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques

L'utilisateur doit être parfaitement conscient que tout traitement opéré sur des données à caractère personnel (données susceptibles d'identifier une personne) est soumis à une règlementation très stricte et que le non-respect de celle-ci l'expose à des sanctions pénales.

Ainsi, le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les règles posées par la loi informatique et libertés du 6 janvier 1978 modifiée, constitue une infraction[27].

5.3 Les obligations du responsable de traitement

Le responsable de traitement est la personne qui détermine les finalités et les moyens du traitement.

Le responsable de traitement est tenu de procéder à une collecte loyale et licite, étant précisé que les finalités de la collecte doivent être déterminées, explicites et légitimes. En toute hypothèse, la collecte doit respecter le principe de proportionnalité : les données collectées doivent être adéquates, pertinentes et non excessives au regard des finalités annoncées. En toute hypothèse, les données doivent être exactes, complètes, mises à jour et conservées pour une durée déterminée.

L'attention de l'utilisateur est attirée sur le fait qu'il existe des règles particulières concernant certaines catégories de données dites « sensibles ». Ainsi, toute collecte de données à caractère personnel qui fait apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui est relative à la santé ou à la vie sexuelle de celles-ci, est interdite.

[27] CP. art. 226-16.

Indépendamment de ce qui précède, il appartient au responsable de traitement de procéder, avant tout traitement de données à caractère personnel, aux formalités requises auprès de la Commission nationale de l'informatique et des libertés (Cnil).

Ainsi, selon le type de traitement ou de données, il s'agira, soit de réaliser une déclaration (ou une déclaration simplifiée) auprès de la Cnil, soit d'obtenir une autorisation de celle-ci. A noter que certains traitements sont exempts de ces formalités et en particulier lorsqu'un correspondant à la protection des données à caractère personnel est nommé.

Le responsable de traitement est tenu, de surcroît de :

- corriger les données collectées inexactes ou incomplètes au regard des finalités pour lesquelles elles ont été collectées ;
- conserver les données sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ;
- assurer la sécurité et la confidentialité des données à caractère personnel, y compris dans le cas où le traitement serait sous-traité à un tiers, ce dernier devant présenter des garanties suffisantes formalisées dans un contrat écrit [28];
- informer, la personne dont les données ont été collectées :
  - de l'identité du responsable de traitement ;
  - de la finalité du traitement ;
  - du caractère obligatoire ou facultatif des réponses ;
  - des conséquences d'un défaut de réponse ;
  - des destinataires des données ;
  - de l'existence d'un droit d'accès, de rectification et d'opposition sur les données les concernant ;
  - le cas échéant, des transferts de telles données vers des pays tiers à l'Union européenne.

6 LES REGLES EN MATIERE D'UTILISATION DES MOYENS DE CRYPTOLOGIE

L'utilisateur est informé de la possibilité d'utiliser les moyens de chiffrement ou de cryptologie autorisés par le SDIS 04 sous réserve du respect des exigences et des conditions d'intégrité et de confidentialité fixées par le SDIS 04.

La mise en œuvre de systèmes de cryptologie est recommandée tant au titre de la sécurité dans la transmission de données que de la preuve de ces mêmes données.

---

[28] L'article 35 de la loi n°78-17 énonce en effet que :
« Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.
Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi.
Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.
Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement ».

L'utilisateur est informé que l'utilisation de moyens de chiffrement ou de cryptologie est strictement réglementée et que les règles édictées ont un caractère impératif tant pour la sécurité, que pour l'intégrité et la confidentialité des informations.

L'utilisation de moyens de cryptologie recouvre différentes fonctions :

- l'authentification des messages ;
- le respect de leur intégrité ;
- la confidentialité des messages ;
- la non répudiation des messages émis, c'est-à-dire l'impossibilité de les remettre en cause.

L'utilisation de moyens de cryptologie ou de chiffrement est libre.

En revanche, la fourniture, le transfert depuis un Etat membre de l'Union européenne ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à déclaration préalable au Premier ministre, sauf exceptions.

Le transfert vers un Etat membre de l'Union européenne et l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à autorisation du Premier ministre, sauf dérogations.

7 LE RESPECT DES LOIS ET REGLEMENTS EN VIGUEUR

Les utilisateurs sont informés que les règles légales et réglementaires en vigueur susvisées s'appliquent dans le cadre de l'utilisation des ressources informatiques du SDIS 04.

En conséquence, les utilisateurs devront notamment respecter, sans que cette liste ait un caractère exhaustif, l'ensemble des règles susvisées.

8 LA MISE A DISPOSITION DU PRESENT GUIDE ET EVOLUTION

Le présent guide est mis à la disposition des utilisateurs sur l'Intranet et/ou par remise matérielle.

Le présent guide sera régulièrement mis à jour et il appartient à l'utilisateur de prendre connaissance de toute nouvelle version du guide qui sera portée à sa connaissance par le biais de la messagerie, par Intranet ou par une remise matérielle.

REPUBLIQUE FRANCAISE

- - - - - - -

Département des Alpes de Haute-Provence

- - - - - - -

Service départemental d'incendie et de secours

COMMUNICATION N° 2020-01 [FIN]

Date de convocation : 19 février 2020
Nombre d'élus en exercice : 5
Présents : 3
Absents : 2
Votants : 3
Réception en Préfecture le :
Délibération certifiée exécutoire le :

EXTRAIT DU REGISTRE

DES COMMUNICATIONS DU BUREAU

DU CONSEIL D'ADMINISTRATION

DU SERVICE DEPARTEMENTAL D'INCENDIE ET DE SECOURS

DES ALPES DE HAUTE-PROVENCE

L'an deux mille vingt et le 25 juin le Bureau du Conseil d'administration du Service départemental d'incendie et de secours s'est réuni au lieu habituel de ses séances, après convocation légale, sous la présidence de Monsieur Pierre POURCIN.

Etaient présent(e)s : Monsieur Robert GAY, 1er vice-président ; monsieur Serge SARDELLA, membre du Bureau.
Etaient excusé(e)s : Madame Geneviève PRIMITERRA, 2ème vice-présidente, monsieur Bernard DIGUET, 3ème vice-président.

Objet : Délégation pour attribuer les marchés publics à procédure adaptée (MAPA inférieurs à 90 000 € HT)

Le Président POURCIN expose :

Par délibération n° 2017-72 du 30 novembre 2017, le Président du conseil d'administration est autorisé, pour la durée de son mandat, à prendre toute décision concernant la préparation, la passation, l'exécution et le règlement des marchés de travaux, de fournitures ou de service passés selon une procédure adaptée. L'avis simple de la Commission d'Appel d'Offres est nécessaire au préalable s'agissant de la signature des marchés publics et accords-cadres à procédure adaptée d'un montant inférieur à 90 000 € HT.

En application de l'article L.1424-30 du Code général des collectivités territoriales, le Président du Conseil d'Administration, représentant légal de l'établissement public, rend compte à l'organe délibérant des décisions qu'il a prises concernant la préparation, la passation, l'exécution et le règlement des marchés et accords-cadres de travaux, fournitures et services, passés selon la procédure adaptée en raison de leur montant ou de leur nature.

Dans le cadre de cette délégation les marchés publics suivants ont été attribués, après négociation :

1) **Marché à procédure adaptée relatif à l'installation de portails automatiques à la DDSIS – montant prévisionnel du marché 50 000,00€ HT**

Lot	Entreprise attributaire	Montant HT
Lot unique	SARL Clotures de Provence 298 Chemin des Colles 83 440 Tourrettes	50 788€

Le Bureau du Conseil d'administration a pris acte de cette communication.

Le Président du Conseil d'administration

Pierre POURCIN