

ARRÊTÉ N° 2002/07/01
DU 20 JUIN 2002 MODIFIÉ

OBJET **Règlement intérieur du service départemental-métropolitain d'incendie et de secours et du corps départemental et métropolitain de sapeurs-pompiers**

Le président du conseil d'administration du service départemental-métropolitain d'incendie et de secours,

Vu le code général des collectivités territoriales et notamment les articles L 1424-1 à L 1424-50, L 1424-69 à L 1424-76 ; R 1424-1 à R 1424-55 ; R 1424-57 ;

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

Vu la loi n° 84-53 du 26 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique territoriale ;

Vu le Code de la sécurité intérieure ;

Vu le Code du service national ;

Vu la loi n° 96-370 du 3 mai 1996 relative au développement du volontariat dans les corps de sapeurs-pompiers ;

Vu la loi n° 2004-811 du 13 août 2004 de modernisation de la sécurité civile ;

Vu la loi n° 2011-851 du 20 juillet 2011 relative à l'engagement des sapeurs-pompiers volontaires et à son cadre juridique ;

Vu les arrêtés n° 04/12/02 du 8 décembre 2004, n° 06/05/04 du 12 mai 2006, n° 06/12/03 du 18 décembre 2006, n° 09/06/04 du 26 juin 2009, n° 11/12/01 du 12 décembre 2011, n° 13/12/02 du 16 décembre 2013, n° 15/12/03 du 18 décembre 2015, n° 16/06/01 du 24 juin 2016, n° 17/02/03 du 24 février 2017, n°18/05/02 du 26 juin 2018 et n°19/05/01 du 27 juin 2019 ;

ARRÊTE

Article 1^{er}: Le règlement intérieur fixant les modalités de fonctionnement du service départemental-métropolitain d'incendie et de secours, et du corps départemental et métropolitain de sapeurs-pompiers et les obligations de service de ses membres est établi ainsi qu'il suit :

TITRE I : DISPOSITIONS GENERALES

Chapitre 1.1 : Application du règlement intérieur

Article 1.1.1 :

Le service départemental-métropolitain d'incendie et de secours (SDMIS) est composé des personnels suivants :

- des sapeurs-pompiers professionnels (SPP),
- des sapeurs-pompiers volontaires (SPV),
- des sapeurs-pompiers professionnels et volontaires membres du service de santé et de secours médical (SSSM),
- des personnels administratifs, techniques et spécialisés (PATS).

Article 1.1.2 :

Le corps départemental et métropolitain est composé des personnels suivants :

- des sapeurs-pompiers professionnels (SPP),
- des sapeurs-pompiers volontaires (SPV),
- des sapeurs-pompiers professionnels et volontaires membres du service de santé et de secours médical (SSSM).

Article 1.1.3 :

Le directeur départemental et métropolitain des services d'incendie et de secours, chef du corps départemental et métropolitain, a autorité sur l'ensemble des personnels composant le service départemental-métropolitain d'incendie et de secours, et le corps départemental et métropolitain. L'ensemble des officiers, sous-officiers et gradés du corps départemental et métropolitain, ainsi que les membres de la hiérarchie PATS participent à l'application du présent règlement intérieur. En cas de non-respect de ces règles, les personnels s'exposent à des sanctions disciplinaires.

Article 1.1.4 :

Un arrêté conjoint du préfet et du président du conseil d'administration du SDMIS fixe, après avis du conseil d'administration, l'organisation du service départemental-métropolitain d'incendie et de secours, et du corps départemental et métropolitain de sapeurs-pompiers.

Article 1.1.5 :

Le règlement intérieur est applicable à tous les personnels du service départemental-métropolitain d'incendie et de secours, et du corps départemental et métropolitain de sapeurs-pompiers.

Article 1.1.6 :

Le règlement intérieur est applicable à toute personne accédant aux locaux du service.

Chapitre 1.2 : Déontologie et obligation de neutralité

Article 1.2.1

Chaque agent et sapeur-pompier volontaire du SDMIS exerce ses fonctions avec dignité, impartialité, intégrité et probité. Dans l'exercice de leurs fonctions, les personnels sont tenus à l'obligation de neutralité. Ils exercent leurs fonctions dans le respect du principe de laïcité. A ce titre, ils s'abstiennent notamment de manifester, dans l'exercice de leurs fonctions, leurs opinions religieuses. Ils traitent de façon égale toutes les personnes et respectent leur liberté de conscience et leur dignité.

Article 1.2.2 :

Afin de préserver la neutralité du service public et, pour les sapeurs-pompiers, les valeurs et traditions qu'incarne l'uniforme, les personnels doivent exclure, durant l'exercice de leurs fonctions, le port de toute inscription ou tout insigne de quelque nature que ce soit, en dehors de ceux prévus dans les tenues d'uniformes telles que définies dans le présent règlement.

Le sapeur-pompier doit s'attacher à paraître, en toutes circonstances, dans une tenue réglementaire et fixée par le chef du corps départemental et métropolitain ou son représentant en respectant l'uniforme qu'il porte, les valeurs et traditions qu'il incarne.

Article 1.2.3 :

Dans le même esprit, les véhicules et bâtiments, et de manière générale l'ensemble des biens mobiliers et immobiliers appartenant au SDMIS, ne peuvent servir de support à des inscriptions et slogans.

Chapitre 1.3 : Obligations de réserve et de discrétion professionnelle

Article 1.3.1 :

Les personnels sont tenus à l'obligation de réserve dans le cadre de l'exercice de leur fonction.

Article 1.3.2 :

Ils doivent faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice ou à l'occasion de l'exercice de leurs fonctions.

Article 1.3.3 :

Ils doivent respecter le secret professionnel dans le cadre des règles instituées dans le code pénal et le code de la santé publique.

Article 1.3.4 :

Dans l'exercice de ses fonctions ou dans les locaux de service, il est formellement interdit à tout agent et sapeur-pompier volontaire du SDMIS de tenir des propos insultants, outrageants, diffamatoires, discriminatoires à caractères raciste, xénophobe, sexiste, relatifs à l'état de santé ou au handicap à l'égard de toute personne, qu'il s'agisse d'un autre agent ou d'un sapeur-pompier volontaire de l'établissement ou d'un tiers.

Toute discrimination, directe ou indirecte, fondée sur l'ethnie, la race, la religion, les convictions, l'âge, le handicap, les activités syndicales, l'orientation sexuelle, le sexe, la grossesse, la maternité et le congé maternité est formellement interdite par la loi. Elle est passible de poursuites pénales.

Article 1.3.5 :

Dans l'exercice des fonctions ou dans les locaux de service, tout acte de harcèlement moral ou sexuel est strictement interdit.

Article 1.3.6 :

Les propos et contenus diffusés sur internet et sur tout support multimédia (forums et listes de discussion, réseaux sociaux, sites internet, blogs...), aussi bien dans le cadre du service que dans la sphère privée, ne doivent porter atteinte ni à l'image, ni à la réputation du SDMIS, ni à chacun de ses personnels.

Chapitre 1.4 : Protection fonctionnelle des personnels

Article 1.4.1 :

Le SDMIS est tenu d'assurer la protection fonctionnelle de ses personnels contre les menaces, violences, voies de fait, injures, diffamations ou outrages qu'ils peuvent subir dans l'exercice de leurs fonctions ou à la suite d'accidents en service commandé dont ils pourraient être victimes.

Chapitre 1.5 : Usage des matériels du SDMIS

Article 1.5.1 :

L'utilisation des matériels appartenant au SDMIS est réservée à un usage exclusivement de service. Toute autre utilisation doit obligatoirement faire l'objet d'une autorisation délivrée par la hiérarchie. Le vol, le détournement ou l'utilisation de matériels appartenant au SDMIS à des fins privées et non autorisées par la hiérarchie exposent les auteurs des faits à des poursuites disciplinaires et, le cas échéant, à des poursuites judiciaires.

Article 1.5.2 :

La messagerie électronique de l'intranet est réservée à un usage de service excluant pour chaque agent et sapeur-pompier volontaire tout usage étranger à son domaine de compétence professionnelle et à ses missions au sein du service.

L'usage à titre privé en est toléré dans des limites raisonnables en fréquence et en volume.

Tout message s'adressant à un groupe de destinataires doit être validé par la hiérarchie.

Afin que tout utilisateur de l'intranet puisse accéder à ces sites, les associations et syndicats liés au SDMIS peuvent demander le référencement de leurs sites internet sur l'intranet Point Eclair en respectant certaines contraintes techniques.

Les informations de Point Eclair n'étant destinées qu'à un usage interne, les utilisateurs de cet outil sont astreints à l'obligation de réserve et à la discrétion professionnelle.

Article 1.5.3 :

L'utilisation des moyens informatiques, téléphoniques et de communication électronique du SDMIS est régie par la charte d'utilisation des moyens informatiques, téléphoniques et de communication électronique.

Conformément aux dispositions légales « Informatique et libertés », cette charte est consultable par tous les personnels sur le site intranet du SDMIS.

Article 1.5.4 :

L'administration des systèmes d'information et de communication du SDMIS est réservée aux personnels habilités par la direction du SDMIS.

Elle est régie par la charte administrateurs des systèmes d'information, annexée à la charte d'utilisation des moyens informatiques, téléphoniques et de communication électronique.

Conformément aux dispositions légales « Informatique et libertés », cette charte est consultable par tous les personnels sur le site intranet du SDMIS.

Chapitre 1.6 : Locaux et moyens de services : définition et accès

Article 1.6.1 :

Sont considérés comme des locaux de service l'ensemble des locaux, y compris les chambres de veille, aires extérieures, parkings, terrains d'exercices et de sport.

Sont considérés comme moyens de service l'ensemble des moyens matériels mis à disposition des agents et des sapeurs-pompiers volontaires pour l'exécution du service (notamment véhicules, bureaux, postes informatiques et accessoires, vestiaires à EPI, téléphonie et logiciels).

Article 1.6.2 :

L'ensemble des locaux et moyens de service doit pouvoir être accessible en permanence à la hiérarchie à l'exception des locaux et panneaux syndicaux autorisés.

Article 1.6.3 :

L'accès aux locaux de service n'est autorisé qu'aux personnels du SDMIS de service et notamment pendant les périodes de gardes, d'astreintes, de permanences, et de temps de travail fonctionnel.

L'accès aux locaux de service par des personnels du SDMIS en dehors de leur temps de service est soumis à l'autorisation de la hiérarchie. Dans ce cas, ces personnels sont soumis à l'intégralité des dispositions du règlement intérieur. L'accès aux locaux de service de toute personne extérieure au SDMIS est soumis à l'autorisation préalable de la hiérarchie.

L'accès aux locaux informatiques des casernes et des sites de l'état-major est réservé aux administrateurs du GSI. Pour des raisons majeures ou sur demande expresse du GSI, cet accès peut être autorisé ponctuellement.

Ces dispositions pourront faire l'objet, le cas échéant, de notes de service d'application.

Article 1.6.4 :

Les chambres de veille ne peuvent être occupées que la nuit, une heure après la prise de garde du soir et jusqu'à 9 heures 30 le lendemain matin.

Elles peuvent être utilisées par les personnels de garde les samedis, dimanches et jours fériés à partir de 12 heures.

Article 1.6.5 :

Lorsque le local de réception de l'alerte d'une caserne défini à l'annexe 2 de l'arrêté préfectoral portant règlement opérationnel et de la caserne logistique, est équipé d'un coin-repos avec lit, un sapeur-pompier de la garde opérationnelle de nuit y est obligatoirement affecté, à la place d'une affectation en chambre de veille.

Article 1.6.6 :

Lorsque les repas de la Sainte-Barbe sont organisés dans les locaux de service, ces locaux de service doivent être libérés au plus tard à 19h00.

Chapitre 1.7 : Conduite des véhicules du SDMIS

Article 1.7.1 :

Les personnels titulaires de permis de conduire sont tenus :

- dans le cas de permis nécessitant un renouvellement de validité, de veiller à ce que leur permis soit toujours en règle. Cette procédure, à respecter scrupuleusement, correspond à une démarche individuelle, placée sous la responsabilité de l'agent ou du sapeur-pompier volontaire - de faire un retour d'information à leur hiérarchie dès lors que leur permis de conduire est validé par l'autorité préfectorale,
- de signaler immédiatement à leur hiérarchie directe toute modification concernant la validité de leur permis de conduire (suspension, retrait de permis, ...).

Article 1.7.2 :

Les agents et sapeurs-pompiers volontaires appelés à conduire un véhicule de service doivent être en possession de l'original de leur permis. L'original de ce permis doit pouvoir être présenté à tout instant à la hiérarchie.

Article 1.7.3 :

La conduite des véhicules du SDMIS est une obligation de service pour tous les sapeurs-pompiers, ainsi que pour les PATS dont l'emploi le nécessite.

Pour la bonne organisation du service et en cas de carence de candidats, le SDMIS peut imposer à un agent ou sapeur-pompier volontaire l'obligation de conduite des véhicules de service. De la même façon, le SDMIS peut interdire à un agent ou sapeur-pompier volontaire la conduite des véhicules de service.

Article 1.7.4 :

En dehors des situations citées dans les articles 1.7.5 et 1.7.6, aucune dérogation au code de la route n'est acceptée.

Cette conduite sans dérogations s'applique :

- à tous les véhicules n'étant pas d'intérêt général prioritaire au sens du code de la route,
- aux véhicules d'intérêt général prioritaire, pour tous les trajets qui ne sont pas spécifiés dans les articles 1.7.5 et 1.7.6 (sauf ordre contraire du CTA/CODIS). On y trouve notamment le retour du centre hospitalier à la caserne ou le retour directement du lieu d'intervention à la caserne,
- aux véhicules quels qu'ils soient, lors du trajet jusqu'à la caserne du sapeur-pompier volontaire alerté par le CTA pour assurer un départ.

Article 1.7.5 :

Des dérogations au sens de l'article R 432-1 au code de la route sont autorisées pour les véhicules d'intérêt général prioritaire dans les cas justifiés par l'urgence de leur mission, sous réserve qu'ils fassent usage simultanément de la signalisation lumineuse (gyrophare) et sonore (deux tons), et toujours sous réserve de rester maître de son véhicule et de ne pas mettre en danger les autres usagers de la route.

On entend par cas justifiés par l'urgence de leur mission :

- les trajets « aller » d'opération de secours sauf pour les trajets « aller » d'intervention pouvant être différés dans le temps (certaines interventions hyménoptères...), de la caserne ou du lieu de départ au site d'intervention ;
- les réengagements des engins par le CTA/CODIS pour une nouvelle intervention ;
- certains déplacements liés aux opérations de secours et sur demande ou après accord du CTA/CODIS.

Article 1.7.6 :

Des dérogations au sens de l'article 4321-1 au code de la route plus limitées sont autorisées pour les véhicules d'intérêt général prioritaire lors du transport de la victime du lieu d'intervention jusqu'au centre hospitalier, car elle comporte également une notion d'urgence.

Dans ces cas, et sous réserve qu'il fasse usage de la signalisation lumineuse (feux de route et gyrophare), et toujours sous réserve de rester maître de son véhicule et de ne pas mettre en danger les autres usagers, les dérogations, plus limitées que dans le cas précédent, seront précisées par note de service et/ou directive opérationnelle.

Sur ordre du CTA/CODIS ou du chef d'agrès ou après avis éventuel du médecin ou d'un infirmier protocolé, le mode de conduite peut appliquer les dispositions de l'article 1.7.5 si le degré d'urgence le justifie.

Article 1.7.7 :

Dans les modes de conduite cités en 1.7.5 et 1.7.6, les obligations suivantes demeurent :

- le port de la ceinture de sécurité est obligatoire dans tous les véhicules du SDMIS, sauf en cas d'absence d'un tel équipement. En outre, il convient d'utiliser en priorité les places équipées de ceintures de sécurité. Le chef d'agrès s'assurera du respect de cette obligation. Il pourra être dérogé de façon exceptionnelle au port de la ceinture de sécurité lorsque la mission le justifie et dès lors que le chef d'agrès l'a autorisé et en a informé le conducteur pour que ce dernier adapte sa conduite en conséquence,
- il n'y a pas de dérogation aux sens interdits, sauf sur décision du conducteur en cas de force majeure lors de l'intervention et sous réserve de ne pas mettre en danger les tiers, le chef d'agrès pouvant s'opposer à cette manœuvre,
- il n'y a aucune dérogation aux feux rouges clignotants des passages à niveaux,
- le retour d'intervention dans les voies de bus et avec les feux de croisement avec avertisseur lumineux est toléré,
- la vitesse des véhicules de plus de 3,5T de Poids Total Autorisé en Charge ou de Poids Total Roulant Autorisé est strictement limitée à 90 km/h, et ce quel que soit le type de voie et de situation opérationnelle. En outre, un dépassement de la vitesse autorisée de 20 km/h en agglomération paraît être un maximum raisonnable pour la sécurité des intervenants et des tiers,
- s'agissant du tramway, toute intersection entre la voie du tramway en site propre et les autres voies de circulation doit être considérée comme équipée de feux tricolores au rouge pour les pompiers. En conséquence, le passage des carrefours se fera en marche prudente, avertisseurs sonores et lumineux actionnés, en capacité de pouvoir stopper à tout moment. Il est en outre déconseillé de dépasser une rame (vitesse tramway 40 km/h et conducteur du tramway sans rétroviseurs) et il est impossible (largeur insuffisante) ou très dangereux de croiser et doubler une rame en station.

Article 1.7.8 :

Quel que soit le type de conduite, le chef d'agrès a l'obligation de faire respecter les règles de prudence au conducteur. Tout manquement constaté d'un conducteur devra faire l'objet d'un rapport du chef d'agrès à sa hiérarchie.

En outre, il convient d'utiliser en priorité, lorsqu'elles sont équipées de ceinture de sécurité, les places assises situées dans la cabine de conduite du véhicule.

Article 1.7.9 :

Le conducteur a obligation de rendre compte des accrochages qu'il aurait eus avec un véhicule du SDMIS, et de remplir un constat d'accident, même en l'absence d'implication d'un tiers.

Article 1.7.10 :

Tout personnel du SDMIS étant amené à conduire des véhicules du SDMIS doit respecter la charte du bon conducteur, accessible à tous sur le réseau intranet du SDMIS.

Article 1.7.11 :

Concernant ce chapitre, le directeur du SDMIS pourra être amené à préciser ou à compléter par notes de service et/ou directives opérationnelles ces règles de conduite.

Chapitre 1.8 : Hygiène et sécuritéArticle 1.8.1 :

Chaque agent et sapeur-pompier volontaire du SDMIS doit veiller à sa sécurité et à sa santé ainsi qu'au respect des règles d'hygiène et de sécurité définies (règlement intérieur, notes de service, consignes, etc..). Chaque agent et sapeur-pompier volontaire doit veiller à la sécurité des autres personnels mais également à celle des tiers (public, usagers).

Tous les personnels du SDMIS doivent tenir compte de l'état de vigilance imposé par leurs missions.

Cet état peut être altéré notamment par une prise d'alcool, de médicaments ou de substances diverses, voire de maladie.

Article 1.8.2.1 :

La hiérarchie relève immédiatement de ses fonctions tout agent ou sapeur-pompier volontaire dont le comportement semble incompatible avec l'exercice de ses missions. L'incompatibilité est constatée notamment lorsque l'un des symptômes suivants est apparent : trouble de l'élocution, trouble de l'équilibre, excitation anormale, prostration, etc...

Article 1.8.2.2 :

Tout personnel qui constate un tel comportement doit en référer immédiatement à la hiérarchie de l'intéressé, sans délai.

Article 1.8.3 :

Pour les sapeurs-pompiers, le service de santé et de secours médical (SSSM) sera immédiatement tenu informé pour assurer la prise en charge et le suivi médical de l'agent ou du sapeur-pompier volontaire relevé de ses fonctions.

En cas d'impossibilité de la part du SSSM, il sera fait appel à un médecin extérieur au SDMIS afin d'assurer la prise en charge de l'agent concerné.

Pour les PATS, un médecin ou le cas échéant le service de santé et de secours médical (SSSM) sera immédiatement tenu informé pour assurer la prise en charge et le suivi médical de l'agent ou du sapeur-pompier volontaire relevé de ses fonctions.

Article 1.8.4 :

L'introduction, la consommation et la distribution de boissons alcoolisées sont strictement interdites dans les locaux de service ou pendant les heures de travail et notamment pendant les périodes de gardes et de travail fonctionnel.

Article 1.8.5 :

Pour tous les personnels du SDMIS, le taux d'alcoolémie maximum toléré dans les locaux de service ou pendant les heures de service est celui fixé par les dispositions du code de la route.

Article 1.8.6 :

A l'occasion des fêtes des 13 et 14 juillet, le directeur départemental et métropolitain peut autoriser des bals à l'intérieur des locaux de service, sous réserve de la signature préalable d'une convention. Cette convention sera établie chaque année avant le 1^{er} avril et devra être signée par le DDMSIS, le chef de caserne concerné et l'organisateur de la manifestation.

Cette convention comportera deux volets :

- Un volet sur l'organisation du bal proprement dite les 13 et 14 juillet, pour lequel les trois signataires devront se mettre d'accord sur les modalités d'accès et d'organisation, le programme, les invitations, etc...
- Un volet concernant l'autorisation de vente et de consommation d'alcool de 2^{ème} catégorie (vin, bière et cidre) qui pourront être autorisées en dérogation exceptionnelle aux dispositions du règlement intérieur sous réserve que l'organisateur s'engage à prendre des mesures actives de prévention contre les excès alcooliques, en accord avec le chef de caserne.

Le respect des règles et la bonne tenue de la manifestation précédente conditionneront l'autorisation et les termes de la convention suivante.

En tout état de cause, les ventes et la consommation d'alcool seront limitées dans la fourchette maximale de 21h à 2h du matin.

Ces ventes et cette consommation d'alcool devront s'effectuer dans un total respect des dispositions législatives et réglementaires en vigueur, notamment celles concernant les mineurs.

Ces ventes et cette consommation d'alcool s'effectueront sous la responsabilité civile et pénale de l'association organisatrice.

Les sapeurs-pompiers de service ainsi que les sapeurs-pompiers en tenue sont astreints à l'intégralité des dispositions du règlement intérieur, sans dérogation aux règles liées à la consommation d'alcool.

Les sapeurs-pompiers de service et ceux participant à l'organisation de la manifestation devront être en tenue de sapeur-pompier et respecter la note de service en vigueur sur l'habillement ou dans une tenue prévue dans la convention mentionnée au présent article.

Article 1.8.7 :

Il est interdit de fumer ou vapoter dans tous les locaux du SDMIS. Compte tenu de l'activité spécifique du SDMIS, cette interdiction est également valable à l'intérieur des véhicules du service, et pendant les interventions.

Toutefois, dans ce dernier cas, pour les sapeurs-pompiers, le chef d'agrès, sous sa responsabilité, pourra autoriser son équipage à fumer ou vapoter, après s'être assuré que toutes les conditions d'hygiène et de sécurité sont réunies. Cette tolérance ne s'applique pas à l'intérieur des véhicules de service.

Article 1.8.8 :

L'introduction, la consommation et la distribution de produits ou mélanges de produits stupéfiants ou psychotropes sont strictement interdites sur le lieu et pendant les heures de service.

Article 1.8.9 :

Les personnels ne doivent pas être sous l'influence des produits cités dans l'article 1.8.8 pendant le temps de service, excepté pour des médicaments résultant d'une prescription médicale dont le service de médecine professionnelle compétent a eu connaissance.

Article 1.8.10 :

Pour les sapeurs-pompiers, et pour les personnels affectés sur certains postes de travail, pour des raisons d'hygiène et de sécurité :

- le port de bijoux apparents (dont les boucles d'oreilles et les piercings) n'est pas autorisé;
- les cheveux doivent être d'une longueur compatible avec le port d'une coiffe ou être attachés;

Afin de garantir une étanchéité efficace et éviter toute fuite de nature à mettre en danger le sapeur-pompier et tout agent concerné, conformément à la doctrine nationale relative à la prévention contre les risques de toxicité liés aux fumées d'incendie, l'équipement de protection respiratoire doit impérativement être porté sur une peau rasée (une pilosité même courte est incompatible avec ce port). De fait :

- le port de la barbe et des favoris est interdit pour les sapeurs-pompiers et les personnels devant porter un équipement de protection respiratoire,
- le rasage est impératif pour la prise de service.

Article 1.8.11 :

Pour des raisons d'hygiène liées aux interventions de secours à personnes, les sapeurs-pompiers veilleront à leur hygiène corporelle.

Article 1.8.12 :

Un protocole soumis à l'avis du comité d'hygiène, de sécurité et des conditions de travail précisera les actions de prévention qui pourront être menées, ainsi que les éventuels contrôles. L'analyse des risques et des accidents survenus devra également être réalisée.

Article 1.8.13 :

Les modalités de mise en œuvre de ce chapitre peuvent être précisées par note de service.

Chapitre 1.9 : Equipements de protection individuelle (EPI) – Habillement et port des tenues d'uniforme

Article 1.9.1 :

Pour exercer leurs missions, le SDMIS met à la disposition des sapeurs-pompiers et des autres personnels affectés sur certains postes de travail des équipements de protection individuelle (EPI). Tout usage des EPI en dehors des missions autorisées par la hiérarchie est formellement interdit. Les sapeurs-pompiers reçoivent également une dotation initiale d'habillement à leur entrée au corps départemental et métropolitain.

Ces EPI appartiennent au service et leur localisation au sein de chaque entité fait l'objet d'une traçabilité.

En cas de suspension d'activité, de cessation d'activité, de mutation ou de départ en retraite, les EPI doivent être rendus immédiatement au chef d'entité.

A titre dérogatoire, après 20 années de service minimum, un agent cessant son activité ou partant en retraite peut solliciter, via sa hiérarchie et après accord du directeur, de conserver son dernier casque.

Article 1.9.2 :

Le détail de la composition des tenues et équipements de protection individuelle (EPI), leurs modalités de dotation, de renouvellement, de réintégration après usage, ainsi que les règles d'utilisation, d'entretien, de maintenance et de formation pour la mise en œuvre des EPI, sont définis par note de service.

Pour les tenues d'uniforme et les effets d'habillements, les conditions d'entretien et de restitution sont définies aux titres II, III et IV.

Article 1.9.3 :

Les sapeurs-pompiers sont astreints, pendant la période de service, au port de l'une des tenues réglementaires définies par les textes en vigueur, sauf autorisation accordée par la hiérarchie.

Article 1.9.4 :

Le port de la tenue opérationnelle de base (ensemble de port permanent), sans équipement de protection individuelle (EPI), est obligatoire pour les sapeurs-pompiers de garde affectés à un départ en intervention lors des rassemblements de prise de garde. Pour les autres rassemblements, la tenue sera adaptée à l'activité à réaliser.

Le port de la tenue d'intervention incendie, avec équipement de protection individuelle, à l'exception de l'appareil respiratoire isolant, est obligatoire pour les personnels de garde affectés à un départ en intervention lors des rassemblements de prise de garde, pour les dates commémoratives et les dates particulières fixées par note de service.

Chaque sapeur-pompier devra remiser ses EPI dans l'espace réservé à cet effet pendant la durée de sa garde.

Les EPI ne doivent en aucune façon sortir de leur entité de rattachement ni être échangés entre agents ou sapeurs-pompiers volontaires, du fait de l'obligation de traçabilité, sauf autorisation de la hiérarchie notamment pour le suivi des actions de formation.

Le vol, le détournement ou l'utilisation de matériels appartenant au SDMIS à des fins privées et non autorisées par la hiérarchie pourront donner lieu à des poursuites disciplinaires et, le cas échéant, exposent le ou les auteurs des faits à des poursuites judiciaires.

Article 1.9.5 :

Le port de la tenue en dehors des périodes de service est interdit pour les sapeurs-pompiers, sauf autorisation accordée par la hiérarchie.

Article 1.9.6 :

Le port des galons est obligatoire pour les sapeurs-pompiers.

Article 1.9.7 :

Le port de tout insigne, attribut ou décoration non réglementaire est prohibé.

Article 1.9.8 :

Le port de l'uniforme impose des contraintes spécifiques.

A ce titre, les coupes et couleurs de cheveux, maquillages et tatouages apparents doivent être compatibles avec l'exercice des fonctions de sapeur-pompier et ne doivent pas attenter à la discrétion ainsi qu'au devoir de réserve du porteur de la tenue.

Article 1.9.9 :

Le port de lunettes de soleil discrètes et sans éléments décoratifs est autorisé en service, notamment pour la conduite, en phase de surveillance ou de progression en zone à forte réverbération solaire. Elles ne sont pas autorisées lors des cérémonies officielles ou, sauf exception, lors des opérations de relations publiques ou médiatiques. Ces restrictions ne concernent pas les verres correctifs, changeant de couleur avec la luminosité ambiante, prescrits pour des raisons médicales.

Article 1.9.10 :

Les PATS sont astreints pendant la période de service au port des équipements de protection individuelle si l'exercice de leur mission l'exige, sauf autorisation accordée par la hiérarchie.

Article 1.9.11 :

Les modalités de mise en œuvre de ce chapitre peuvent être précisées par note de service.

Chapitre 1.10 : Surveillance médicale

Article 1.10.1 :

La surveillance médicale des agents et des sapeurs-pompiers volontaires est obligatoire. Elle est exercée par les médecins du service de santé et de secours médical pour les sapeurs-pompiers et par un service de médecine professionnelle et préventive du travail pour les PATS.

Chapitre 1.11 : Affectation temporaire

Article 1.11.1 :

Les personnels peuvent être affectés temporairement dans une autre caserne, groupement ou service à tout moment, de manière exceptionnelle, pour faire face à une défaillance imprévisible.

Chapitre 1.12 : Relations du service avec les associations de sapeurs-pompiers

Article 1.12.1 :

Le fonctionnement des associations de sapeurs-pompiers à l'intérieur des locaux du SDMIS est placé sous la responsabilité des présidents d'associations.

Il doit être compatible avec les dispositions du règlement intérieur.

Article 1.12.2 :

Toutes les manifestations, et en particulier les fêtes traditionnelles organisées par les associations, à l'intérieur des locaux de service, sont soumises à l'autorisation préalable de la hiérarchie.

L'organisateur de ces manifestations doit se conformer, d'une part, aux obligations légales réglementaires, et, d'autre part, à l'intégralité des dispositions du règlement intérieur. Les invitations de personnes extérieures et le programme de ces manifestations doivent être validés par la hiérarchie.

Article 1.12.3 :

Les modalités de mise en œuvre de ce chapitre pourront être précisées par note de service.

Chapitre 1.13 : Usage de matériel électronique personnel :

Article 1.13.1 :

L'usage de matériel électronique personnel dans le cadre du service (notamment lecteur de musique, téléphones et ordinateurs portables personnels...) est toléré pendant les heures de travail, sauf avis contraire de la hiérarchie. Cependant, des restrictions ou des interdictions peuvent être précisées par note de service et/ou directive opérationnelle pour des raisons de sécurité ou d'intérêt du service.

La connexion au système d'information du SDMIS des appareils professionnels ou personnels (ordinateurs, tablettes, ordiphones, etc...) n'appartenant pas à la flotte du SDMIS est réglementée par la charte d'utilisation des moyens informatiques, téléphoniques et de communication électronique. Elle est soumise à l'autorisation préalable expresse de la direction et à l'acceptation par l'agent ou le sapeur-pompier volontaire des pré-requis techniques et des conditions d'utilisation définis par le groupement des systèmes d'information.

Chapitre 1.14 : Prise et/ou diffusion d'images et de sons en opérations de secours et en service

Hormis la réalisation d'images (photos, vidéos) ou la prise de sons effectués pour les besoins de service avec des moyens mis à disposition des intervenants par le SDMIS (caméras mobiles, drones, tablettes, téléphones ...), toute prise d'images ou de sons lors d'opérations de secours et en service avec des appareils personnels ainsi que leur diffusion sont strictement interdites sauf autorisation expresse de la hiérarchie.

Chapitre 1.15 : Image du SDMIS :

L'enregistrement de données (images, sons, ...) dans les locaux de service est interdit sauf autorisation de la hiérarchie.

Toute utilisation de l'image du SDMIS, de ses locaux, matériels et bâtiments, nécessite un accord préalable de la hiérarchie. La diffusion ou la reproduction de documents et de logos, propriétés du SDMIS, est soumise à autorisation préalable de la hiérarchie. Les documents sont soumis au droit de la propriété intellectuelle.

TITRE II : DISPOSITIONS APPLICABLES AUX SAPEURS-POMPIERS PROFESSIONNELS

Chapitre 2.1 : Cumul d'activité

Article 2.1.1 :

Tout sapeur-pompier professionnel doit consacrer l'intégralité de son activité professionnelle aux tâches qui lui sont confiées.

Article 2.1.2 :

Il ne peut exercer, à titre professionnel, une autre activité lucrative de quelque nature que ce soit, sauf dérogations fixées par les textes en vigueur et éventuellement précisées par délibération du conseil d'administration du SDMIS.

Chapitre 2.2 : Régime de travail

Article 2.2.1 :

Le régime de travail est défini par le conseil d'administration du SDMIS.

Chapitre 2.3 : Obligations de service

Article 2.3.1 :

Les services de sécurité constituent une obligation de service ; ils sont définis par directives opérationnelles.

Article 2.3.2 :

Les contrôles et les procédures applicables dans les casernes doivent être réalisés dans des conditions permettant de s'assurer de :

- la performance opérationnelle des équipes,
- la sécurité des personnels et notamment l'utilisation des équipements de protection individuelle,
- la maintenance des matériels et des moyens opérationnels,
- l'entraînement physique et sportif.

Ces contrôles et ces procédures constituent des obligations de service. Ils peuvent être précisés par la hiérarchie.

Article 2.3.3 :

Des reconnaissances opérationnelles des points d'eau incendie destinées à vérifier leur disponibilité opérationnelle sont réalisées aux dates fixées par la hiérarchie en application des dispositions du règlement départemental et métropolitain de défense extérieure contre l'incendie. Elles permettent

également, si nécessaire, la mise à jour des plans d'interventions des communes et des établissements répertoriés, ainsi que des fichiers informatiques d'envoi des secours.

Article 2.3.4 :

Les exercices dans les établissements à risques, tels les établissements recevant du public, les immeubles de grande hauteur et les établissements industriels soumis à plans de secours, doivent être effectués suivant les programmes arrêtés par la hiérarchie.

Article 2.3.5 :

La formation spécifique au CTA-CODIS 69 constitue une obligation de service et est fixée par la hiérarchie sur la base de ces principes.

Article 2.3.6 :

L'entretien professionnel annuel est un droit pour chaque SPP.

Article 2.3.7 :

L'exercice des spécialités est une obligation de service. Elle est définie par la hiérarchie en fonction des besoins de service et des conditions d'aptitudes médicale et physique des sapeurs-pompiers professionnels concernés.

Article 2.3.8 :

En cas de circonstances exceptionnelles qui feraient obstacle, à raison par exemple de l'insuffisance des personnels présents, à l'exécution du service public de protection de la sécurité des personnes et des biens, les sapeurs-pompiers professionnels devront se rendre disponibles sans délai dès lors qu'ils auront été informés par le SDMIS de l'existence de telles circonstances. Cette information sera faite notamment par voie de message téléphonique ou courriel préétabli ou de SMS adressé sur le téléphone portable communiqué préalablement et spontanément au service et ce, afin de permettre une couverture opérationnelle adaptée à de telles circonstances. Ces mesures ne portent pas préjudice à l'application des dispositions relatives à l'organisation du service en cas de grève (note de service n° 2015-071 du 1^{er} octobre 2015).

Chapitre 2.4 : Formations

Article 2.4.1 :

La formation individuelle constitue une obligation réglementaire.

Article 2.4.2 :

Tous les sapeurs-pompiers professionnels doivent accomplir 5 jours de formation continue par an indépendamment de la formation permanente assurée directement dans les casernes. Cette durée, qui constitue un minimum, constitue également un maximum hors les cas de formations spécifiques liées à l'avancement.

Toute durée supérieure à cette norme doit faire l'objet d'une décision formelle de l'autorité hiérarchique. C'est notamment le cas pour les spécialités.

Chapitre 2.5 : Parcours professionnels

Section 1 : Pour l'ensemble des SPP

Article 2.5.1.1 :

La mobilité au sein du corps, facteur de progrès, fait partie de la carrière des sapeurs-pompiers.

Pour l'ensemble des sapeurs-pompiers professionnels de tous grades, la mobilité peut intervenir à tout moment dans l'intérêt du service ou sur demande de l'agent.

Article 2.5.1.2 :

La mobilité intervient également pour les besoins du service, suivant les modalités définies ci-après. Dans ce cas, elle fait préalablement l'objet d'avis de vacance de poste.

Section 2 : Les sapeurs-pompiers professionnels non-officiers

En complément de la section 1 :

Article 2.5.2.1 :

Pour les besoins du service, la mobilité intervient dès lors qu'un sapeur-pompier est depuis plus de 10 ans dans une même caserne ou service. Des dérogations à cette règle peuvent être apportées dans l'intérêt du service.

Article 2.5.2.2 :

Elle intervient également à l'occasion des changements de grade de sergents ou d'adjudants. Cependant, dans l'intérêt du service, notamment lié aux spécialités, des dérogations peuvent être apportées.

Article 2.5.2.3 :

Au cours de sa carrière, un sapeur-pompier professionnel non-officier, dès lors qu'il a cinq ans d'ancienneté au moins, doit effectuer, en fonction des besoins du service, un passage de 2 à 3 ans, soit au CTA-CODIS 69, soit au groupement formation-école départementale et métropolitaine. Des affectations pour des durées de 5 à 6 ans, en fonction des besoins du service, sont possibles au CTA-CODIS 69 ou au groupement-formation-école départementale et métropolitaine. En fonction des besoins du service et à la demande de l'agent, une affectation d'une durée supérieure est envisageable, tant au CTA-CODIS 69 qu'au groupement formation-école départementale et métropolitaine.

Section 3 : Les sapeurs-pompiers professionnels officiers

En complément de la section 1

Sous section 3.1 : Les lieutenants et capitaines.

Article 2.5.3.1.1 :

Pour les besoins du service, la mobilité intervient dès lors qu'un lieutenant ou un capitaine est depuis plus de 5 ans dans une même caserne ou groupement. Des dérogations à cette règle peuvent être apportées dans l'intérêt du service.

Article 2.5.3.1.2 :

Elle intervient également à l'occasion des changements aux grades de lieutenants et de capitaines. Des dérogations à cette règle peuvent être apportées dans l'intérêt du service.

Sous section 3.2 : Les commandants, lieutenants-colonels et colonels.

Article 2.5.3.2.1 :

La mobilité peut intervenir à tout moment dans l'intérêt du service.

Chapitre 2.6 : Exercice du droit syndical

Article 2.6.1 :

Afin de garantir les principes de continuité du service public et d'exercice du droit syndical, les représentants syndicaux sollicitant une décharge d'activité de service, ou une autorisation d'absence pour raison syndicale, devront dans la mesure du possible en faire la demande écrite à la hiérarchie au moins 3 jours à l'avance.

Article 2.6.2 :

Inscrit dans le préambule de la constitution, le droit de grève s'exerce dans un cadre législatif et réglementaire enrichi par la jurisprudence. Celui-ci confie au chef de service la responsabilité du bon fonctionnement du service public, et à ce titre, il appartient à ce dernier d'opérer la conciliation nécessaire entre la défense des intérêts professionnels, dont la grève constitue l'une des modalités, et la préservation de l'intérêt général auquel elle peut porter atteinte.

Principes généraux :

Pour permettre la mise en place d'un service adapté assurant la continuité du service public :

- Le directeur départemental et métropolitain des services d'incendie et de secours ou son représentant désignera, par avance, les agents strictement nécessaires en nombre et en qualification,
- Les modalités sont définies par note de service.

Article 2.6.3 :

En période de grève, tout sapeur-pompier désigné ou maintenu en service est tenu de respecter l'ensemble des dispositions du présent règlement.

Chapitre 2.7 : Congés

Article 2.7.1 :

Les congés annuels d'été des sapeurs-pompiers opérationnels non officiers sont répartis sur 3 périodes de 21 jours consécutifs pendant les vacances scolaires. Il sera tenu compte de la priorité donnée aux chargés de famille, par la réglementation en vigueur.

Article 2.7.2 :

Les congés annuels d'été des autres sapeurs-pompiers sont répartis selon la réglementation en vigueur, dans la limite des nécessités imposées par la continuité du service public.

Article 2.7.3 : Le SDMIS facilitera la prise de congés pendant les vacances scolaires.

Article 2.7.4 :

Congés maladie

Par tout moyen à leur convenance, les agents doivent informer sans délai leur hiérarchie de leur absence, de la prolongation de celle-ci, ainsi que de leur reprise afin de permettre l'organisation du travail en leur absence.

Ils doivent obligatoirement adresser à la direction des ressources humaines les volets 2 et 3 du certificat d'arrêt de travail (ou document équivalent) dans un délai de 48h à compter de la date d'établissement du certificat médical.

Ils doivent conserver le volet 1 (ou document équivalent portant les mentions médicales) qui pourra leur être demandé par tout médecin agréé dans le cadre de la médecine professionnelle, le contrôle, l'aptitude ou l'appui d'une demande de congé longue maladie ou longue durée.

Chapitre 2.8 : Habillement

Article 2.8.1 :

Les sapeurs-pompiers professionnels bénéficient d'une masse annuelle de tenues d'uniforme et d'effets d'habillement.

Article 2.8.2 :

Les sapeurs-pompiers professionnels quittant le corps départemental et métropolitain, par voie de mutation, doivent restituer leurs tenues.

Chapitre 2.9 : Remplacement des absences non programmables

Article 2.9.1 :

Afin d'assurer la continuité du service public et de maintenir le potentiel opérationnel, la hiérarchie pourra faire appel :

- d'abord aux sapeurs-pompiers de l'équipe de renfort.

La garde de ces sapeurs-pompiers est établie en complément de la programmation trimestrielle des casernes. A ce titre, ces sapeurs-pompiers peuvent être, en cas de besoin, affectés temporairement dans une autre caserne.

- puis aux sapeurs-pompiers d'autres casernes, en priorisant dans la limite de l'organisation du service les sapeurs-pompiers qui se porteraient volontaires.

TITRE III : DISPOSITIONS APPLICABLES AUX SAPEURS-POMPIERS VOLONTAIRES

Chapitre 3.1 : Disponibilité

Article 3.1.1 :

Les sapeurs-pompiers volontaires doivent faire preuve de disponibilité pour les activités organisées par le service. La hiérarchie de la caserne veillera à la mise en oeuvre de ces dispositions.

Article 3.1.2 :

Les chefs de groupement et les chefs de caserne veilleront à garantir la disponibilité opérationnelle des casernes placées sous leurs responsabilités.

La disponibilité opérationnelle peut être organisée sous forme de garde dans les centres mixtes, ainsi que dans les casernes organisées avec des gardes à la parution du présent règlement.

Article 3.1.3 :

Les sapeurs-pompiers volontaires qui effectuent des gardes postées doivent faire preuve de disponibilité opérationnelle en dehors des périodes de garde postée.

Chapitre 3.2 : Tâches obligatoires

Article 3.2.1 :

Les services de sécurité auxquels participent les sapeurs-pompiers volontaires sont définis par directives opérationnelles.

Article 3.2.2 :

Les contrôles et les procédures applicables dans les casernes doivent être réalisés dans des conditions permettant de s'assurer de :

- la performance opérationnelle des équipes,
- la sécurité des personnels, notamment l'utilisation des équipements de protection individuelle,
- la maintenance des matériels et des moyens opérationnels,
- l'entraînement physique et sportif.

Ces contrôles et ces procédures, qui conditionnent la sécurité et la capacité opérationnelle des sapeurs-pompiers volontaires, sont organisés par la hiérarchie.

Article 3.2.3 :

Des reconnaissances opérationnelles des points d'eau incendie destinées à vérifier leur disponibilité opérationnelle sont réalisées aux dates fixées par la hiérarchie en application des dispositions du règlement départemental et métropolitain de défense extérieure contre l'incendie. Elles permettent également, si nécessaire, la mise à jour des plans d'interventions des communes et des établissements répertoriés, ainsi que des fichiers informatiques d'envoi des secours.

La réalisation des reconnaissances opérationnelles des points d'eau incendie, lorsqu'elles sont confiées à des sapeurs-pompiers volontaires, est programmée par le chef de caserne en fonction de leur disponibilité.

Article 3.2.4 :

Les exercices dans les établissements à risques, tels les établissements recevant du public, les immeubles de grande hauteur et les établissements industriels soumis à plans de secours, doivent être effectués suivant les programmes arrêtés par la hiérarchie.

Chapitre 3.3 : Formation

Article 3.3.1 :

La formation initiale, la formation de maintien et de perfectionnement des acquis constituent une obligation réglementaire. Le sapeur-pompier volontaire s'engage à acquérir et à maintenir les compétences nécessaires et adaptées à l'accomplissement des missions qui lui sont confiées.

Article 3.3.2 :

Les durées des formations suivies par les sapeurs-pompiers volontaires sont fixées par arrêté du président du conseil d'administration du SDMIS après avis du comité consultatif départemental des sapeurs-pompiers volontaires.

Chapitre 3.4 : Mobilité

Article 3.4.1 :

La mobilité des sapeurs-pompiers volontaires au sein du corps départemental et métropolitain est soumise à l'autorisation du directeur départemental et métropolitain des services d'incendie et de secours, après avis des chefs de caserne et des chefs de groupements concernés.

Chapitre 3.5 : Habillement

Article 3.5.1 :

Pour le renouvellement et l'entretien des tenues d'uniforme et effets d'habillement, une dotation est prévue dans chaque caserne.

Article 3.5.2 :

Les sapeurs-pompiers volontaires quittant le corps départemental et métropolitain doivent restituer leurs tenues d'uniforme et effets d'habillement sauf si la cessation d'activité intervient après 20 ans de service.

Chapitre 3.6 : Saisonniers

Article 3.6.1 :

Les demandes d'engagement en tant que sapeur-pompier volontaire saisonnier dans un autre département sont soumises à l'autorisation de la hiérarchie.

Article 3.6.2 :

Pendant la période d'engagement, la responsabilité du SDMIS est dérogée ; le sapeur-pompier volontaire n'est pas autorisé à utiliser le matériel de protection individuelle fourni par le SDMIS.

Chapitre 3.7 : Remplacement des absences non programmables

Article 3.7.1 :

Afin d'assurer la continuité du service public et de maintenir le potentiel opérationnel, la hiérarchie pourra faire appel :

- d'abord aux sapeurs-pompiers de l'équipe de renfort

La garde de ces sapeurs-pompiers est établie en complément de la programmation trimestrielle des casernes. A ce titre, ces sapeurs-pompiers peuvent être, en cas de besoin, affectés temporairement dans une autre caserne.

- puis aux sapeurs-pompiers d'autres casernes, dans la limite de l'organisation du service les sapeurs-pompiers qui se porteraient volontaires.

Chapitre 3.8 : Affectation temporaire

Article 3.8.1 :

Les sapeurs-pompiers volontaires peuvent être affectés temporairement dans une autre caserne à tout moment, de manière exceptionnelle, pour faire face à une défaillance imprévisible.

Chapitre 3.9 : Maladie et accident du travail

Article 3.9.1 :

Tout sapeur-pompier volontaire placé en arrêt maladie ou accident du travail au titre de son activité professionnelle doit déclarer sa situation au SDMIS.

Pendant la durée de son arrêt maladie ou de son accident du travail, il ne peut exercer une activité au SDMIS. Il est tenu d'en rendre compte immédiatement au service qui, dès lors prend les dispositions adéquates.

Chapitre 3.10 : Création des comités intercentres

Article 3.10.1 :

Il est créé un comité intercentres par groupement territorial. Certaines attributions du comité consultatif départemental des sapeurs-pompiers volontaires peuvent être déléguées aux comités intercentres selon les dispositions réglementaires du code de la sécurité intérieure. La composition et les modalités de désignation et de fonctionnement des comités intercentres sont fixées par arrêté du président du conseil d'administration.

Chapitre 3.11: Représentation du service et promotion du volontariat

Article 3.11.1 :

Chaque sapeur-pompier volontaire s'engage à avoir un comportement respectueux de l'image des sapeurs-pompiers, tant au sein du service que dans le cadre de sa vie privée. Il contribue, notamment par son attitude, à promouvoir cet engagement citoyen afin d'en assurer la pérennité. Il s'engage, dans la mesure de sa disponibilité, à participer aux cérémonies publiques et à représenter le service.

TITRE IV : DISPOSITIONS PARTICULIERES APPLICABLES AU SERVICE DE SANTE ET DE SECOURS MEDICAL (SSSM)

Chapitre 4.1 : Dispositions applicables aux personnels membres du SSSM

Article 4.1.1 :

Les dispositions du titre II sont applicables aux sapeurs-pompiers professionnels membres du SSSM.

Article 4.1.2 :

Les dispositions du titre III sont applicables aux sapeurs-pompiers volontaires membres du SSSM.

Article 4.1.3 :

Les dispositions du titre V sont applicables aux PATS affectés au SSSM.

Chapitre 4.2 : Dispositions complémentaires applicables aux personnels membres du SSSM

Article 4.2.1 :

En application de l'article R1424-26 alinéa 3 du CGT, les professionnels de santé membres du service de santé et de secours médical sont placés sous l'autorité du médecin-chef et, pour les missions exercées par le service ou la caserne dans lesquels ils sont affectés, ils relèvent du chef de ce service ou caserne.

Article 4.2.2 :

Le médecin-chef adjoint, outre les responsabilités qui lui sont confiées à titre permanent, assiste le médecin-chef, et assume les fonctions du médecin-chef et ses prérogatives en l'absence de celui-ci.

Article 4.2.3 :

Article abrogé

Article 4.2.4 :

Article abrogé

Article 4.2.5 :

Article abrogé

TITRE V : DISPOSITIONS APPLICABLES AUX PERSONNELS ADMINISTRATIFS, TECHNIQUES ET SPECIALISES (PATS)

Chapitre 5.1 : Cumul d'activité

Article 5.1.1 :

Tout PATS doit consacrer l'intégralité de son activité professionnelle aux tâches qui lui sont confiées.

Article 5.1.2 : (Créé par l'arrêté n° 06/12/03 du 18 décembre 2006, modifié par l'arrêté n°15/12/03 du 18 décembre 2015)

Il ne peut exercer à titre professionnel une autre activité lucrative de quelque nature que ce soit, sauf dérogations fixées par les textes en vigueur et éventuellement précisées par délibération du conseil d'administration du SDMIS.

Chapitre 5.2 : Régime de travail

Article 5.2.1 :

Le régime de travail est défini par le conseil d'administration du SDMIS.

Chapitre 5.3 : Obligations de service

Article 5.3.1 :

L'accomplissement des missions fixées par la hiérarchie constitue une obligation de service.

Article 5.3.2 :

L'entretien professionnel annuel est un droit pour chaque agent.

Chapitre 5.4 : Formation

Article 5.4.1 :

Les agents bénéficient d'un droit à la formation dans la limite des contraintes du service.

Article 5.4.2 :

Pour des raisons de services, la formation peut aussi constituer une obligation.

Chapitre 5.5 : Parcours professionnels

Article 5.5.1 :

L'affectation dans une direction, un groupement ou service est fixée par le directeur départemental et métropolitain des services d'incendie et de secours en fonction des postes ouverts par avis de vacance, et du profil de l'agent.

Article 5.5.2 :

Pour l'ensemble des PATS, la mobilité peut intervenir à tout moment dans l'intérêt du service ou sur demande de l'agent.

Article 5.5.3 :

La mobilité peut s'avérer nécessaire en cas d'avancement de grade notamment dans le cas où l'accès au grade concerné n'est pas possible dans le service d'affectation de l'agent.

Chapitre 5.6 : Exercice du droit syndical

Article 5.6.1 :

Afin de garantir les principes de continuité du service public et d'exercice du droit syndical, les représentants syndicaux sollicitant une décharge d'activité de service, ou une autorisation d'absence pour raison syndicale, devront dans la mesure du possible en faire la demande écrite à la hiérarchie au moins 3 jours à l'avance.

Article 5.6.2 :

En cas de grève, le directeur départemental et métropolitain des services d'incendie et de secours prendra toutes les mesures utiles pour assurer un service adapté garantissant la continuité du service public.

Article 5.6.3 :

En période de grève, tout PATS désigné ou maintenu en service est tenu de respecter l'ensemble des dispositions du présent règlement.

Chapitre 5.7 : Congés

Article 5.7.1 :

Les congés annuels sont répartis selon la réglementation en vigueur, dans la limite des nécessités imposées par la continuité du service public.

Article 5.7.2 :

Le SDMIS facilitera la prise de congés pendant les vacances scolaires.

Article 5.7.3 :

En cas d'absence pour maladie, les agents doivent, par tout moyen à leur convenance, informer sans délai leur hiérarchie de leur absence, de la prolongation de celle-ci, ainsi que de leur reprise afin de permettre l'organisation du travail en leur absence.

Ils doivent obligatoirement adresser à la direction des ressources humaines les volets 2 et 3 du certificat d'arrêt de travail (ou document équivalent) dans un délai de 48h à compter de la date d'établissement du certificat médical.

Ils doivent conserver le volet numero 1 (ou équivalent) qui pourra leur être demandé par tout médecin agréé dans le cadre de la médecine professionnelle, le contrôle, l'aptitude ou l'appui d'une demande de congés longue maladie ou longue durée.

Chapitre 5.8 : Habillement

Article 5.8.1 :

Les PATS quittant le SDMIS, par voie de mutation, doivent restituer leurs tenues.

Article 2 : Le directeur départemental et métropolitain des services d'incendie et de secours est chargé de l'exécution du présent arrêté qui sera publié au recueil des actes administratifs du service départemental-métropolitain d'incendie et de secours.

Fait à Lyon, le DATÉ

Le président du conseil d'administration du
service départemental-métropolitain
d'incendie et de secours

SIGNÉ

Charte du bon conducteur

Le conducteur d'un véhicule du SDMIS doit être par son comportement en toutes circonstances un ambassadeur de la sécurité routière.

Je reconnais être ce type de conducteur et je m'engage, outre le respect de la réglementation, du code de la route et des autres usagers :

- A être titulaire d'un permis de conduire en cours de validité et adapté à l'engin que je suis amené à conduire. Je m'engage à faire connaître à ma hiérarchie les restrictions dont il peut faire l'objet (suspension, problème médical...);
- A ne conduire qu'en pleine possession de mes moyens et de mes capacités afin de ne pas engager ma vie, ni celle des autres. Je m'engage à ne pas conduire sous l'emprise d'alcool, de médicaments psycho-actifs ou de produits stupéfiants ;
- A veiller au bon état général de mon véhicule ;
- A boucler ma ceinture de sécurité dans mon véhicule et demander à mes collègues de faire de même ;
- A rester maître de mon véhicule et ne pas mettre en danger la vie d'autrui ;
- A respecter les restrictions de circulation lors de conditions climatiques difficiles ;
- A ne pas faire usage d'un téléphone portable en main en conduisant.

SDMIS

SAPEURS-POMPIERS

CHARTRE

**UTILISATEURS - UTILISATION DES
MOYENS INFORMATIQUES,
TELEPHONIQUES ET
DE COMMUNICATION ELECTRONIQUE**

Table des matières

GENERALITES	3
Chapitre 1 – Objectifs	3
Chapitre 2 – Champ d’application	3
2.1. Opposabilité	3
2.2. Moyens et services concernés	3
2.3. Usages concernés	4
REGLES D’UTILISATION	4
Chapitre 3 – Règles de bon usage	4
3.1. Généralités	4
3.2. Messagerie	4
3.3. Internet	5
Chapitre 4 – Accès et Identification	5
4.1. Accès aux locaux techniques	5
4.2. Identifiant et mot de passe personnels	5
Chapitre 5 – Mobilité	6
5.1. Nomadisme	6
5.2. Accès à distance	7
5.3. Accès WiFi	7
5.4. Télétravail	7
5.5. Gestion des supports amovibles	7
5.6. Utilisation de matériels personnels à des fins professionnelles	8
Chapitre 6 - Nature de l’utilisation / Droit d’accès	8
6.1. Utilisation professionnelle	8
6.2. Utilisation non-professionnelle résiduelle	9
6.3. Droit d’accès	10
Chapitre 7 – Disponibilité	10
Chapitre 8 – Confidentialité des données	10
Chapitre 9 – Gestion des Ressources informatiques	11
9.1. Affectation des droits	11
9.2. Départ de l’Utilisateur	11
9.3. Absence de l’Utilisateur	11
Chapitre 10 – Principes de sécurité	12
10.1. Obligation de vigilance	12
10.2. Comportement de l’Utilisateur en cas d’atteinte potentielle à la sécurité	13
Chapitre 11 – Protection de la propriété intellectuelle	13
Chapitre 12 – Protection des données à caractère personnel	14
12.1. Données à caractère personnel concernant les Utilisateurs	14
12.2. Données à caractère médical	14
12.2.1. Dossiers médicaux individuels des personnels du SDMIS	14
12.2.2. Données à caractère médical collectées dans le cadre d’une alerte	15
12.2.3. Accès des Utilisateurs à des Données à caractère personnel	15
CONTROLE ET MAINTENANCE	15
Chapitre 13 – Mesures de contrôle	15
Chapitre 14 – Opérations de maintenance	16
Chapitre 15 – Conservation des données	16
Chapitre 16 – Sanctions	17
MODALITES D’APPLICATION	17
Chapitre 17 – Entrée en vigueur	17
GLOSSAIRE	18

GENERALITES

Les termes Utilisateurs, Ressources informatiques, Administrateur, Hiérarchie, Cloud, GSI, Données à caractère personnel, Nomades sont définis dans le glossaire à la fin de la présente charte.

Chapitre 1 – Objectifs

1. Cette charte s'applique aux Utilisateurs amenés à créer, consulter et utiliser les Ressources informatiques du Service départemental-métropolitain d'incendie et de secours (ci-après le « SDMIS »).
2. Elle a pour objet de fixer les règles d'utilisation des Ressources informatiques du SDMIS. La présente charte pourra évoluer en fonction du contexte légal et réglementaire et de la politique de sécurité applicable au sein du SDMIS. Le bon usage et l'utilisation réglementaire des outils du Système d'Information (ci-après le « SI ») peuvent être régentés par des Conditions Générales d'Utilisation (ci-après les « CGU ») qui compléteront les dispositions de la présente charte.
3. Les règles ainsi définies sont destinées à assurer un niveau optimum de disponibilité, d'intégrité, de confidentialité et de traçabilité des Ressources informatiques, et d'une manière générale le respect des dispositions légales et réglementaires applicables.
4. La présente charte est rédigée dans l'intérêt de chaque Utilisateur et manifeste la volonté du SDMIS d'assurer un usage loyal, sécurisé et responsable des Ressources informatiques.
5. Elle a pour objectif de formaliser les règles de déontologie et de sécurité que les Utilisateurs s'engagent à respecter, en faisant usage des Ressources informatiques.
6. La présente charte tient compte des recommandations de la Commission Nationale de l'Informatique et des Libertés (ci-après la « CNIL »), du Forum des Droits sur l'Internet et de l'Agence Nationale de la Sécurité des Systèmes d'Information (ci-après l'« ANSSI »).
7. La présente charte pourra évoluer en fonction du contexte légal et réglementaire et de la politique de sécurité applicable au sein du SDMIS.

Chapitre 2 – Champ d'application

2.1. Opposabilité

8. La présente charte constitue une annexe au Règlement intérieur du SDMIS et produit, à ce titre, les mêmes effets. Elle est donc opposable, à tout Utilisateur.
9. Toutefois, la présente charte pourra être complétée par des documents spécifiques pour certaines catégories de personnel. Il en est ainsi, notamment, de l'Administrateur, qui sera soumis aux dispositions de la présente charte ainsi qu'à son annexe n°1, la Charte Administrateur.

2.2. Moyens et services concernés

10. Sont visés par la présente charte, l'ensemble des Ressources informatiques :
 - Qui sont la propriété du SDMIS et/ou qui sont mis à la disposition des Utilisateurs à des fins professionnelles ;
 - Qui sont la propriété personnelle de l'Utilisateur, et pour lesquels celui-ci a obtenu une habilitation de la part du SDMIS afin de les utiliser dans le cadre de son activité professionnelle ;

2.3. Usages concernés

11. La présente charte a vocation à s'appliquer quel que soit le lieu d'utilisation des Ressources informatiques.

REGLES D'UTILISATION

Chapitre 3 – Règles de bon usage

3.1. Généralités

12. L'Utilisateur est responsable du bon usage des Ressources informatiques et s'engage à les utiliser dans le respect des règles définies dans la présente charte.

13. L'Utilisateur s'engage à suivre toutes les actions de sensibilisation proposées par le SDMIS sur la sécurité du SI et la protection des données.

14. L'Utilisateur doit prendre soin des Ressources informatiques mis à sa disposition et faire preuve d'une vigilance particulière à leur égard.

15. L'utilisation des Ressources informatiques doit également s'effectuer dans le respect des lois, notamment celles relatives à la propriété intellectuelle et aux publications portant atteinte à la dignité de la personne humaine.

16. A ce titre, l'Utilisateur ne doit en aucune manière se livrer à la consultation, au chargement, au stockage, à la publication ou à la diffusion de fichiers et de messages, dont le contenu présente un caractère injurieux, raciste, pornographique ou diffamatoire, sans que cette liste ne soit exhaustive.

17. Ceci s'applique tant aux fichiers qu'aux messages, avec ou sans pièces attachées, quelle que soit la forme des contenus (notamment sonores, audiovisuels, multimédias ou logiciel).

18. L'Utilisateur doit en conséquence proscrire tout comportement pouvant inciter des tiers à lui adresser de tels documents et les détruire en cas de réception fortuite.

19. De plus, conformément à l'article 1.3.6 du Règlement intérieur, l'Utilisateur s'engage à ce que ses éventuels propos et contenus diffusés sur internet ainsi que sur tout support multimédia (forums et listes de discussion, réseaux sociaux, sites internet, blogs, courriels, etc.), aussi bien dans le cadre professionnel que dans la sphère privée, ne portent pas atteinte à l'image et à la réputation du SDMIS et du corps départemental et métropolitain de sapeurs-pompiers ainsi qu'à chacun de ses membres.

3.2. Messagerie

20. Le SDMIS met à la disposition de l'Utilisateur une adresse de messagerie électronique professionnelle nominative lui permettant d'émettre et de recevoir des messages. Son utilisation est de la responsabilité de l'Utilisateur et doit se faire dans un cadre strictement professionnel. Une utilisation non professionnelle résiduelle est cependant tolérée conformément au sous-chapitre 6.2.

21. Les messages électroniques ont la même portée qu'un courrier manuscrit et peuvent être communiqués à des tiers. Ils peuvent également former un contrat sous certaines conditions (articles 1369-1 à 1369-11 du code civil) ou être utilisés à des fins probatoires. L'Utilisateur doit donc être vigilant dans sa correspondance.

22. Afin d'assurer la sécurité et la performance du service de messagerie, des limitations sont appliquées par le SDMIS sur le format et la taille des pièces jointes ainsi que sur la capacité de stockage de la messagerie.

23. Le SDMIS s'assure de la sauvegarde des courriels et assure un archivage de ceux-ci conformément aux délais légaux. Cependant, l'Utilisateur est informé que la messagerie n'est pas un espace de stockage. Il est de sa responsabilité de stocker sur le réseau du SDMIS les messages et documents ou pièces jointes qu'il souhaite conserver.

24. L'Utilisateur s'engage à sécuriser l'envoi de données sensibles ou confidentielles :

- En évitant de mettre ces données dans le corps du message ;
- En chiffrant les pièces jointes avec l'aide du support du GSI si besoin ;
- En s'assurant de l'adresse des destinataires ;

25. Il est strictement interdit à l'Utilisateur d'envoyer des messages électroniques à l'ensemble du SDMIS sauf en cas de validation préalable de la Direction du SDMIS.

3.3. Internet

26. Le SDMIS met à la disposition de l'Utilisateur un accès à Internet. Son utilisation est de sa responsabilité et doit se faire dans un cadre strictement professionnel. Une utilisation non professionnelle résiduelle est cependant tolérée conformément au sous-chapitre 6.2.

27. L'Utilisateur s'engage à n'utiliser que les navigateurs dûment autorisés et mis à disposition par le SDMIS.

28. L'Utilisateur s'engage à respecter les outils de protection d'accès à Internet mis en place par le SDMIS (filtrage Internet, catégorisation de sites Internet, ...).

29. Il est strictement interdit de stocker des données professionnelles sur des solutions de Cloud (Google Drive, Dropbox, iCloud ou autres) non spécifiquement autorisées par le SDMIS.

30. Le téléchargement sur Internet est uniquement toléré dans un cadre professionnel et doit respecter les droits de la propriété intellectuelle tels que définis dans le chapitre 11. Le SDMIS se réserve le droit de limiter cette pratique (fichier trop volumineux ou présentant un risque sécuritaire).

31. Le streaming sur Internet est uniquement toléré dans un cadre professionnel. Le SDMIS se réserve le droit de limiter son usage en cas de perturbation du bon fonctionnement des Ressources informatiques.

Chapitre 4 – Accès et Identification

4.1. Accès aux locaux techniques

32. L'accès aux locaux techniques est strictement réservé au personnel habilité ou ayant reçu un accord explicite et temporaire de la part du Groupement des Systèmes d'Information (ci-après le « GSI ») ou du Groupement Bâtiments (ci-après le « GBAT »).

33. Pour des raisons de sécurité, l'accès aux locaux techniques peut être conditionné à l'usage de badges ou de clés individuels. De même, il est strictement interdit d'obstruer volontairement la fermeture des différents points d'accès.

4.2. Identifiant et mot de passe personnels

34. Chaque Utilisateur est doté d'un identifiant personnel et d'un mot de passe confidentiel d'accès aux Ressources informatiques qu'il utilise sur le site du SDMIS ou en dehors des locaux du SDMIS.

35. A titre exceptionnel, sur dérogation validée par le RSSI, un accès dérogatoire aux Ressources informatiques sera autorisé par l'intermédiaire d'un compte générique.

36. Pour ne pas être deviné par des logiciels, ce mot de passe doit être suffisamment complexe (combinaison de lettres minuscules et majuscules, de chiffres et de caractères spéciaux) et difficilement identifiable (mot référencé dans le dictionnaire ou en lien avec l'Utilisateur).

37. Dans ce cadre, tout mot de passe doit suivre la politique de gestion des mots de passe du SDMIS et être modifié selon une fréquence déterminée par le SDMIS. Il est recommandé à l'Utilisateur d'utiliser un coffre-fort numérique (tel que Keepass) pour gérer l'ensemble de ses mots de passe.

38. Ce mot de passe est personnel, incessible et temporaire. En conséquence, il est interdit à l'Utilisateur :

- De procéder à la moindre divulgation de son mot de passe ;
- De stocker son mot de passe sur un support physique (comme les post-it) ou dans un fichier informatique ;
- D'autoriser le navigateur à enregistrer son mot de passe ;
- D'utiliser un identifiant autre que le sien, dans l'hypothèse où il en aurait eu connaissance ;
- D'utiliser son mot de passe dans un environnement personnel (messagerie personnelle, services internet en ligne, etc.) ;

39. Sauf à avoir engagé préalablement une demande de suppression ou de suspension, tout usage des Ressources informatiques est réputé avoir été réalisé par le porteur de l'identifiant d'accès qui en assume les conséquences juridiques et financières, sauf à ce qu'il soit en mesure de prouver le contraire.

40. Le SDMIS se réserve, pour quelque raison que ce soit, de manière temporaire ou définitive, le droit d'accorder, de refuser, de modifier ou de supprimer tout ou partie du droit d'accès d'un Utilisateur.

Chapitre 5 – Mobilité

5.1. Nomadisme

41. Les Ressources informatiques ne peuvent pas sortir des locaux du SDMIS sauf si elles sont considérées comme « Nomades » ou sur autorisation écrite du SDMIS.

42. Les Ressources informatiques « Nomades » peuvent être affectées à des Utilisateurs :

- Soit de façon nominative ;
- Soit temporairement dans le cadre de leurs missions et/ou régime de travail spécifique (télétravail) ;

43. Elles restent la propriété du SDMIS. A ce titre, seul le GSI est habilité à assurer leur administration.

44. L'Utilisateur est informé que l'utilisation des Ressources informatiques « Nomades » nécessite des niveaux de surveillance et de confidentialité renforcés et relève de sa responsabilité en termes de vigilance par rapport à la perte ou au vol.

45. A ce titre, l'Utilisateur devra notamment veiller à ce que des tiers non autorisés (collègues, famille, autre personne extérieure au SDMIS) ne puissent pas accéder à ces Ressources informatiques « Nomades », les utiliser ou accéder à leurs contenus.

46. L'Utilisateur devra utiliser les moyens de protection physiques mis à sa disposition (câble de sécurité) pour se protéger contre les potentielles tentatives de vol et respecter les principes de sécurité tels que décrits dans le chapitre 10.

47. Avant toute utilisation de son ordinateur portable en mobilité, l'Utilisateur devra établir une connexion avec le réseau du SDMIS via un Réseau Privé Virtuel (ci-après le « VPN »).

48. Pour le bon fonctionnement des ordinateurs portables, smartphones et tablettes, un minimum d'espace disque, fixé par le SDMIS, doit rester disponible.

49. L'Utilisateur est informé de la mise à disposition par le SDMIS de moyens techniques lui permettant d'exercer son droit à la déconnexion (comme les messages d'absence pour la messagerie ou l'indicateur présentiel pour la messagerie instantanée).

5.2. Accès à distance

50. Lorsqu'un accès à distance est accordé à un Utilisateur, celui-ci s'engage à utiliser les moyens techniques d'authentification qui lui seront remis et aucun autre. En termes de sécurité et de confidentialité, l'Utilisateur est soumis aux mêmes obligations que celles visées pour la gestion des identifiants et devra suivre toutes les prescriptions complémentaires qui lui seront signifiées.

5.3. Accès WiFi

51. Plusieurs accès WiFi sont disponibles au SDMIS :

- Un WiFi est destiné aux Utilisateurs dotés d'une Ressource informatique du SDMIS pour l'accès aux Ressources informatiques du SDMIS ;
- Un WiFi peut être proposé aux agents ou aux personnels tiers du SDMIS pour leurs connexions personnelles à partir de leurs équipements personnels ;

52. L'Utilisateur est informé que la connexion aux différents réseaux WiFi est nominative. A ce titre, l'accès au WiFi est conditionné au respect de la présente charte ;

53. En fonction des usages, le SDMIS se réserve le droit de limiter l'accès à certaines fonctionnalités ainsi que la bande passante.

5.4. Télétravail

54. Dans le cadre du télétravail, l'Utilisateur s'engage :

- À n'utiliser que les Ressources informatiques fournies par le SDMIS ;
- À respecter les principes de sécurité (chapitre 10) et les mesures de contrôle mises en place (chapitre 13) ;

55. Dans le cas où l'octroi de Ressources informatiques est spécifiquement lié à l'exercice du télétravail, celles-ci seront reprises en cas d'arrêt ou d'interruption de longue durée.

5.5. Gestion des supports amovibles

56. L'Utilisateur est autorisé à connecter tout support amovible fourni par le GSI aux Ressources informatiques du SDMIS.

57. Dans ce cadre, ces supports amovibles doivent :

- N'être utilisés que pour le transfert de données et non pour leur stockage ;
- Ne contenir que des données professionnelles ;
- Ne pas être connectés à des Ressources informatiques autres que celles du SDMIS (matériels personnels) ;

58. Il est strictement interdit de brancher intentionnellement sur les Ressources informatiques des supports amovibles portables (disque dur, clé USB, téléphone portable, cigarette électronique, cartes SD, chargeurs, supports proposés dans les hôtels/aéroports, ...) de source inconnue ou dont le degré de confiance de l'Utilisateur est faible.

59. Dans ce cadre et à titre exceptionnel, l'Utilisateur peut sous sa responsabilité connecter :

- Tout support amovible fourni par le SDMIS à des matériels informatiques autres que ceux du SDMIS ;
- Des supports amovibles portables personnels aux Ressources informatiques du SDMIS ;

60. L'Utilisateur s'engage à sécuriser les données sensibles ou confidentielles présentes sur ces supports amovibles en les chiffrant avec l'aide du support du GSI si besoin ;

61. Le SDMIS se réserve le droit de restreindre ou de désactiver certaines fonctionnalités des Ressources informatiques (comme les ports USB) pour éviter que ces dernières ne soient compromises.

5.6. Utilisation de matériels personnels à des fins professionnelles

62. Toute utilisation de matériels personnels est interdite sur des Ressources informatiques du système opérationnel assurant la gestion des opérations de secours.

63. Sauf en cas de situation particulière, les Utilisateurs bénéficiant de Ressources informatiques fournies par le SDMIS s'engagent à ne pas utiliser de matériel personnel de même nature à des fins professionnelles.

64. Le SDMIS laisse la faculté à ses agents d'utiliser leurs matériels personnels dans le cadre de leur activité professionnelle sous réserve du respect de la présente charte et des conditions générales d'utilisation du service concerné.

65. Le GSI peut, à sa discrétion, accorder ou révoquer cet usage.

Chapitre 6 - Nature de l'utilisation / Droit d'accès

6.1. Utilisation professionnelle

66. Les Ressources informatiques sont réservées à un usage professionnel. Une utilisation non-professionnelle résiduelle est cependant tolérée selon le sous-chapitre 6.2.

67. Dans tous les cas, et quelles que soient les conditions effectives d'utilisation, l'usage des Ressources informatiques est présumé avoir un tel caractère.

68. Sont ainsi présumés avoir un caractère professionnel, notamment :

- Les fichiers créés grâce à ces moyens par un Utilisateur, pour l'exécution de son travail.

- Les connexions établies par un Utilisateur sur des sites internet pendant son temps de travail et pour l'exécution de son travail ;

69. Le SDMIS sauvegarde à intervalles réguliers les fichiers stockés sur le réseau. A ce titre, tout document professionnel doit être stocké sur le réseau.

70. Chaque Utilisateur dispose d'un espace nominatif sécurisé au sein duquel des données confidentielles ou non peuvent être stockées. Pour des raisons de continuité de service, l'utilisation de cet espace se fera dans le respect du sous-chapitre 9.3 « Absence de l'utilisateur ».

6.2. Utilisation non-professionnelle résiduelle

71. Toute utilisation de Ressources informatiques du système opérationnel à des fins non-professionnelles est interdite.

72. L'Utilisation des Ressources informatiques à des fins non professionnelles est tolérée sur le SI non opérationnel pour répondre, en cas d'urgence ou de nécessité, à des obligations socialement admises.

73. Cette utilisation doit être exceptionnelle, demeurer raisonnable, tant dans sa fréquence que dans sa durée et doit notamment se faire dans le respect des règles de bon usage (chapitre 3), de confidentialité (chapitre 8) et des principes de sécurité (chapitre 10) de la présente charte.

74. Une telle utilisation ne doit notamment pas :

- Perturber le bon fonctionnement du service et des Ressources informatiques ;
- Compromettre l'activité professionnelle de l'Utilisateur ;
- Porter atteinte à l'image et la confidentialité des données du SDMIS ;
- Être susceptible d'engager la responsabilité du SDMIS ;
- Poursuivre un but lucratif ;

75. La confidentialité attachée à une correspondance non professionnelle doit être indiquée par les mentions « Privé » ou « Personnel » en tête de la zone « objet » du message, afin notamment que le destinataire du message puisse être informé de sa nature. Le recours aux pièces jointes est à éviter.

76. Les messages à caractère privé sont, en tout état de cause, émis et reçus sous la seule responsabilité de l'Utilisateur qui dégage le SDMIS de toute responsabilité.

77. De la même façon, l'Utilisateur peut créer un répertoire informatique, utilisé pour stocker des documents personnels au sein du disque dur de l'ordinateur, sous réserve que le document personnel et le répertoire informatique comportent dans leur nom les termes « Privé » ou « Personnel ». La taille de ce dossier pourra être limitée par le SDMIS. Le stockage de documents personnels est interdit sur tout autre espace de stockage propriété du SDMIS.

78. L'Utilisateur est informé que le SDMIS n'assurera pas le transfert des documents personnels en cas d'échange de Ressources informatiques.

79. Le SDMIS se réserve le droit de limiter ou de suspendre cette tolérance d'utilisation non professionnelle notamment en cas d'abus ou de nécessité technique.

6.3. Droit d'accès

80. Les fichiers informatiques et / ou messages électroniques non identifiés comme étant personnels ou privés dans les conditions définies au sous-chapitre 6.2 sont considérés comme ayant un caractère professionnel.

81. Par conséquent, le SDMIS pourra avoir accès à ces fichiers informatiques et/ou messages électroniques, même en dehors de la présence de l'Utilisateur concerné.

82. En revanche, le SDMIS ne pourra pas avoir accès aux fichiers informatiques et/ou messages électroniques identifiés comme étant personnels ou privés en dehors de la présence et sans le consentement de l'Utilisateur sauf en cas de risque ou d'événement particulier (enquête judiciaire).

Chapitre 7 – Disponibilité

83. Le SDMIS peut interrompre, modifier ou supprimer tout ou partie des Ressources informatiques afin d'assurer le bon fonctionnement du SI (maintenance, traçabilité, optimisation, sécurité, détection des abus, fins statistiques, etc.) de manière temporaire ou définitive, générale et non discriminatoire.

84. Le SDMIS s'efforcera, dans la mesure du possible, de prévenir les Utilisateurs dans des délais raisonnables, notamment en cas de maintenance.

Chapitre 8 – Confidentialité des données

85. Le respect de la confidentialité des données est une exigence essentielle du SDMIS.

86. La confidentialité des données du SDMIS est garantie par une obligation générale et permanente de discrétion et de secret professionnel à l'égard des informations auxquelles l'Utilisateur a accès ou dont il peut prendre connaissance dans le cadre de son activité professionnelle.

87. A cette fin, les Utilisateurs s'engagent notamment à :

- Veiller à ce que les tiers non autorisés par le SDMIS n'aient pas accès à ces données ;
- D'une manière générale, respecter les obligations de discrétion et devoir de réserve attachées à l'exercice de leur fonction.

88. Il est strictement interdit, aux Utilisateurs non habilités, de diffuser la moindre information à caractère professionnel sur le Cloud ou les réseaux sociaux.

89. L'Utilisateur s'engage donc notamment :

- A ne pas divulguer et / ou diffuser des informations relatives aux conditions de travail au sein du SDMIS ;
- A ne pas diffuser de contenus (textes, photos, vidéos) relatifs à ses interventions, sauf accord préalable de la Direction du SDMIS ;
- A ne pas configurer sa boîte de messagerie SDMIS pour transférer automatiquement courriels et pièces jointes d'ordre professionnel vers d'autres comptes de messagerie, notamment personnels ;

90. En tout état de cause, la transmission de données confidentielles, ne peut être réalisée qu'aux conditions suivantes déterminées par la Direction du SDMIS :

- Habilitation de l'émetteur (ou délégation validée par la Direction du SDMIS) ;

- Désignation d'un destinataire autorisé ;
- Respect d'une procédure sécurisée (chiffrement, signature numérique, visa).

Chapitre 9 – Gestion des Ressources informatiques

9.1. Affectation des droits

91. Les droits d'accès d'un Utilisateur aux Ressources informatiques sont soumis à la délivrance d'un compte Utilisateur matérialisé par un nom d'Utilisateur et un mot de passe personnel.

92. Ce compte Utilisateur est personnel, confidentiel et incessible. Il est strictement interdit à l'Utilisateur de masquer sa véritable identité par quelque moyen que ce soit (usurpation d'identité).

93. La Hiérarchie veille à la cohérence entre les droits d'accès autorisés et les missions de l'Utilisateur.

94. L'Utilisateur peut se voir confier des droits d'accès à des espaces collaboratifs plus ou moins restreints (Teams, Sharepoint, ...) dans le cadre de ses missions professionnelles. L'Utilisateur est informé que la présente charte s'applique également à ces espaces.

95. A titre exceptionnel, le GSI peut accorder des droits spécifiques à privilèges à certains Utilisateurs. Ces droits pouvant présenter un risque pour la sécurité du SI, l'Utilisateur s'engage à ne les utiliser que dans les conditions définies par le GSI.

9.2. Départ de l'Utilisateur

96. Lors de son départ définitif du SDMIS, l'Utilisateur doit mettre en place une réponse courriel automatique indiquant qu'il quitte le SDMIS et précisant le contact assurant la continuité du service.

97. Lors de son départ définitif du SDMIS, l'Utilisateur doit remettre, à la Hiérarchie, l'ensemble des Ressources informatiques, les badges et les clés qui lui ont été remis, en bon état général de fonctionnement.

98. Sauf nécessité liée à la continuité du service et pour un temps raisonnable qui ne saurait excéder trois (3) mois, le compte de messagerie de l'Utilisateur est supprimé le jour de son départ.

99. Ses identifiants permettant l'accès aux Ressources informatiques sont également désactivés. Si l'Utilisateur a bénéficié d'un moyen d'authentification à distance, il s'engage à le restituer. En tout état de cause, cet accès à distance sera également désactivé.

100. Le répertoire identifié comme étant personnel, ainsi que tous les documents de même nature, doivent être supprimés par l'Utilisateur au plus tard la veille de son départ du SDMIS.

101. A défaut et sauf procédure judiciaire ou enquête administrative, ces éléments sont automatiquement supprimés le lendemain du départ de l'Utilisateur du SDMIS, sans être consulté et sans qu'aucune copie ne soit réalisée.

102. L'Utilisateur sera destitué de son ou ses numéros de téléphones fixes et/ou mobiles. Ce ou ces numéros pourront être réattribués dès le jour de départ de l'Utilisateur.

9.3. Absence de l'Utilisateur

103. En cas d'absence prolongée planifiée, l'Utilisateur doit mettre en place une réponse courriel automatique. Cette réponse doit indiquer la date de retour au travail et le contact en cas d'urgence.

104. Chaque Utilisateur doit veiller à ce que la continuité du service soit assurée sur le plan des données du SI, conformément aux modalités d'organisation du service et telle que définie par la Hiérarchie.

105. En cas de manquement à cette obligation, et notamment dans l'hypothèse d'une absence de l'Utilisateur pour quelque raison et pour quelque durée que ce soit, le SDMIS se réserve le droit d'accéder directement aux dossiers, répertoires, courriers électroniques et plus généralement tous documents à caractère professionnel de l'Utilisateur.

106. Cette intervention s'effectuera dans le respect de l'utilisation privative des Ressources informatiques, telle que définie au sous-chapitre 6.2 de la présente charte.

Chapitre 10 – Principes de sécurité

10.1. Obligation de vigilance

107. L'Utilisateur s'engage à utiliser les Ressources informatiques de façon loyale et à être vigilant en signalant toute anomalie ou intrusion susceptible de nuire à leur sécurité ainsi qu'à celle du SI du SDMIS.

108. Cette vigilance implique, notamment, le respect des règles de conduite suivantes :

- Quand un courriel est douteux (émetteur inconnu, fautes d'orthographe, motif inhabituel, ...), ne pas ouvrir les pièces jointes et ne pas cliquer sur les liens ;
- Vérifier le nom de tous les destinataires avant d'envoyer un courriel ;
- Envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, afin de ne pas communiquer leurs adresses électroniques à l'ensemble des destinataires ;
- Prendre en compte le risque de retard ou de non remise des courriels et SMS, notamment pour l'envoi des correspondances importantes ;
- Ne pas faire suivre les messages du type « chaîne de solidarité » et les détruire ;

109. En cas de réception de messages non sollicités (spams), l'Utilisateur veille à ne pas les ouvrir, ne pas y répondre, et à envoyer une copie d'écran au support du GSI.

110. De plus, l'Utilisateur est averti de l'existence de règles de gestion des Ressources informatiques. Pour la messagerie, ces règles autorisent le retardement, l'interdiction d'envoi ou encore la suppression de fichiers et de messages (antispam) présentant des risques liés à leur taille ou à leur contenu.

111. Par ailleurs, les Ressources informatiques sont exclusivement installées, configurées et paramétrées par le personnel habilité par le SDMIS.

112. A ce titre, l'Utilisateur s'engage notamment :

- A se conformer et à ne pas tenter de contourner la sécurité et les moyens de surveillance mis en place par le SDMIS (filtrages Internet, chiffrement des disques durs) ;
- A ne pas réaliser de partage de connexion à partir d'un équipement (téléphone, clé Internet) non SDMIS ;
- A ne pas modifier ou désactiver les installations, configurations et paramétrages des Ressources informatiques réalisés par le SDMIS ;

- A systématiquement activer la mise en veille de son écran, protégée par mot de passe, ou à se déconnecter lorsque les Ressources informatiques ne sont plus sous sa surveillance ;
- A ne pas effectuer de tests de sécurité sur le SI du SDMIS ;

113. Pour les documents papier à caractère confidentiel, l'Utilisateur s'engage :

- A retirer immédiatement des imprimantes les documents concernés ;
- A les stocker de façon sécurisée (mise sous clé) en cas d'absence au poste de travail ;
- A procéder à leur destruction définitive ;

10.2. Comportement de l'Utilisateur en cas d'atteinte potentielle à la sécurité

114. L'Utilisateur est tenu d'informer sans délai à la fois la Hiérarchie et le support du GSI de tout dysfonctionnement, altération, perte, vol, destruction, ou toute demande de renseignements abusive venant de l'extérieur, ainsi que de tout autre événement quelle qu'en soit la nature pouvant affecter la sécurité du SI du SDMIS.

En aucun cas, l'Utilisateur ne devra fournir des renseignements relatifs au SI du SDMIS sans autorisation du GSI.

115. Dans l'hypothèse de la survenance d'un des événements précités, l'Utilisateur s'engage à effectuer toutes les démarches (dont notamment un compte rendu de perte, dépôt de plainte, déclaration d'assurance, etc.) qui lui seraient demandées par la Hiérarchie ou le GSI.

116. L'Utilisateur s'engage à contacter le support du GSI s'il détecte qu'il bénéficie de droits d'accès qui ne sont pas en adéquation avec ses missions.

117. Dans l'hypothèse où l'Utilisateur serait invité par la Hiérarchie ou le GSI à prendre des mesures d'urgence ou de sécurité physique, celui-ci s'engage à les appliquer sans le moindre délai.

118. Le remplacement d'une Ressource informatique sera effectué à la discrétion de la Hiérarchie ou du GSI.

Chapitre 11 – Protection de la propriété intellectuelle

119. L'utilisation des Ressources informatiques implique le respect des droits de propriété intellectuelle du SDMIS.

120. A ce titre, l'Utilisateur s'engage notamment à :

- Passer par le support du GSI pour toute installation de logiciel ;
- Utiliser les logiciels mis à sa disposition dans les conditions de la licence souscrite par le SDMIS ;
- Ne pas effectuer de copie illicite de logiciel et, a fortiori, de tenter d'installer des logiciels pour lesquels le SDMIS ne posséderait pas un droit de licence ;
- Ne pas reproduire et utiliser les bases de données, pages web ou autres créations du SDMIS ou de tiers protégés par le droit d'auteur ou un autre droit privatif sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;
- Ne pas diffuser des textes, des images, des photographies, des œuvres musicales ou audiovisuelles et, plus généralement, toute création copiée sur Internet.

Chapitre 12 – Protection des données à caractère personnel

12.1. Données à caractère personnel concernant les Utilisateurs

121. Le SDMIS s'engage à ce que les données concernant les Utilisateurs soient collectées et traitées de manière loyale, proportionnée et licite, dans le respect des dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et Libertés » et du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 - Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit Règlement Général sur la Protection des Données (ci-après le « RGPD »).

122. Les Utilisateurs qui, dans le cadre professionnel, souhaitent collecter ou traiter des Données à caractère personnel doivent prendre contact avec le Délégué à la Protection des Données (ci-après le « DPD »).

123. Les finalités pour lesquelles les données sont traitées sont fondées sur des bases juridiques précisées dans le registre de traitement de Données à caractère personnel. Les Données à caractère personnel sont conservées pour une durée également fixée dans le registre de traitement.

124. Conformément aux dispositions de la loi Informatique et Libertés et du RGPD, les Utilisateurs sont informés que certains outils disposent par défaut d'un indicateur de présence (Skype, Teams, Sharepoint...). Il leur appartient de paramétrer leur statut pour éviter toute intrusion dans leur vie privée.

125. De plus, dans le cadre de la surveillance médicale des agents du SDMIS, telle que prévue à l'article 1.10.1 du Règlement intérieur, les médecins du service de santé et de secours médical du SDMIS sont amenés à connaître des informations relevant du secret médical.

126. A ce titre, ces Utilisateurs doivent en permanence veiller au respect de celui-ci, dans les conditions définies au sous-chapitre *Données à caractère médical* 12.2 de la présente charte.

12.2. Données à caractère médical

12.2.1. Dossiers médicaux individuels des personnels du SDMIS

127. Il est précisé que les ordinateurs et le réseau du service de santé et de secours médical font partie intégrante de la structure informatique du SDMIS. L'ensemble des données informatiques de ce service sont par ailleurs gérées sur un réseau logique indépendant.

128. Conformément à l'article 33 de l'arrêté du 6 mai 2000 fixant les conditions d'aptitude médicale des sapeurs-pompiers professionnels et volontaires et les conditions d'exercice de la médecine professionnelle et préventive au sein des services départementaux d'incendie et de secours, la gestion des dossiers médicaux individuels des Utilisateurs est soumise à une confidentialité absolue.

129. Compte tenu de leur caractère confidentiel, le SDMIS a établi une liste limitative des personnels habilités à accéder à ces dossiers médicaux.

130. A ce titre, tous les éléments liés à la gestion des informations à caractère médical, notamment les dossiers médicaux de santé au travail, ne sont accessibles ni en lecture, ni en écriture aux Utilisateurs autres que ceux expressément habilités par le médecin-chef du SDMIS

131. De la même façon, les personnels pouvant accéder aux ordinateurs et au réseau du service de santé et de secours médical du SDMIS sont habilités par le médecin-chef du SDMIS et font partie de la liste précitée.

132. Il est précisé que ces personnels habilités sont soumis aux dispositions prévues par l'article 226-13 du code pénal, et doivent en tout état de cause respecter leur obligation de secret professionnel.

12.2.2. Données à caractère médical collectées dans le cadre d'une alerte

133. De façon générale, les personnels du SDMIS qui seraient amenés, notamment dans le cadre d'une alerte, à connaître et/ou à partager avec des professionnels de santé des données ou informations à caractère médical concernant une victime, sont soumis au secret professionnel.

134. A ce titre, ils s'engagent notamment à :

- Respecter l'obligation de discrétion professionnelle et du devoir de réserve attachée à leur statut ;
- Respecter la confidentialité de ces données et/ou informations et à ne pas les révéler à des tiers autres que des professionnels de santé ;
- Informer sans délai la Hiérarchie en cas de violation du secret professionnel ;

12.2.3. Accès des Utilisateurs à des Données à caractère personnel

135. Dans le cadre de leur activité, les Utilisateurs qui seraient amenés à avoir accès à des Données à caractère personnel s'engagent à respecter les dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et Libertés » et du RGPD du 16 avril 2016.

136. A ce titre, ils s'engagent notamment à :

- Traiter les Données à caractère personnel uniquement pour la ou les seule(s) finalité(s) prévu(es) dans le registre de traitement de Données à caractère personnel ;
- Aider le SDMIS dans la démarche de mise en conformité au RGPD en prenant en compte les principes de protection des données dès la conception ;

137. Dans ce cadre, il est par ailleurs rappelé que les Utilisateurs sont soumis à une obligation générale de réserve, ainsi qu'à un devoir de discrétion incombant à leur statut.

138. De plus, dans l'hypothèse où un Utilisateur serait amené, dans le cadre de ses fonctions, à avoir accès à des données à caractère médical ou sensibles (origine raciale ou ethnique, orientation sexuelle, appartenance syndicale, politique...), il s'engage à respecter une confidentialité absolue sur ces données.

139. L'Utilisateur notifie sans délai toute violation de Données à caractère personnel après en avoir pris connaissance à sa Hiérarchie ainsi qu'au DPD et au GSI.

CONTROLE ET MAINTENANCE

Chapitre 13 – Mesures de contrôle

140. De par l'activité qui est la sienne, le SDMIS est soumis à une obligation générale de sécurité en application des dispositions du code pénal, relatives à la protection des systèmes de traitement automatisés de données, de la loi Informatique et libertés et du RGPD.

141. A ce titre, 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 (enregistrement des sites Internet visités).

142. Le SDMIS peut diligenter toutes opérations techniques de contrôle permettant de vérifier le respect des dispositions de la présente charte ou des règles légales, soit de sa propre initiative, soit

dans le cadre de procédures judiciaires ou d'enquêtes administratives. Il pourra également procéder à un audit de sécurité du matériel personnel utilisé dans le cadre professionnel, après accord du propriétaire de ce matériel.

143. Dans ce cadre, l'Utilisateur est informé que les Administrateurs peuvent analyser les flux Internet sécurisés, à l'exception :

- Des flux des sites bancaires ;
- Des flux traitant de données personnelles à caractère médical ;
- Des flux de messagerie personnelle (webmail).

144. L'Utilisateur est informé que les smartphones sont géolocalisés afin de pouvoir intervenir en cas de perte ou de vol (effacement des données, blocage d'utilisation d'appareil).

145. Dans ce cadre, l'Utilisateur est informé que les Administrateurs peuvent notamment être amenés à ouvrir, dans sa messagerie, tout message revêtant le caractère professionnel défini dans le sous-chapitre 6.1 et à vérifier l'ensemble des connexions dudit Utilisateur.

146. Lors de ces accès, les Administrateurs sont tenus de respecter la confidentialité des informations, auxquelles ils accèdent.

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

Chapitre 14 – Opérations de maintenance

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

149. Ces opérations de maintenance peuvent nécessiter l'application de mises à jour. L'Utilisateur s'engage à ne pas les interrompre et est informé que les Ressources informatiques peuvent être activées à distance pour les effectuer.

150. Ces opérations de maintenance peuvent nécessiter l'intervention de l'Administrateur, sur site ou sous la forme d'une « prise de main à distance ». La prise de main à distance s'effectue avec accord préalable de l'Utilisateur, ou sans son accord lorsqu'il est absent ou en cas de nécessité absolue de sécurité.

151. A aucun moment l'Utilisateur ne doit donner son mot de passe personnel pour la réalisation des opérations de maintenance par le GSI.

152. L'objectif de ces opérations n'est autre que d'assurer le bon fonctionnement et la sécurité du SI.

153. Afin de garantir une utilisation normale des Ressources informatiques et éventuellement d'identifier les usages contraires aux règles de confidentialité ou de sécurité des données, l'Administrateur peut être amené à prendre connaissance de données ou de messages émis ou reçus par l'Utilisateur, et à examiner le journal de ses connexions.

154. Si, à l'occasion d'opérations de maintenance ou de contrôle, l'Administrateur identifie une utilisation anormale et/ou un contenu illicite ou préjudiciable, il en informe sa Hiérarchie.

Chapitre 15 – Conservation des données

155. Le SDMIS prend en charge la sauvegarde des données informatiques de l'établissement.

156. Chaque Utilisateur doit organiser et mettre en œuvre, selon les instructions de la Hiérarchie ou du GSI, les moyens nécessaires à la conservation des messages lorsque cela est nécessaire.

157. Les traces détaillées d'activité sont conservées pendant les durées légales ou conventionnelles, à l'issue desquelles elles sont détruites.

158. Elles sont considérées comme preuve de l'utilisation des Ressources informatiques par les Utilisateurs. Elles peuvent également faire l'objet d'un traitement statistique anonyme.

159. Ces traces peuvent être communiquées aux autorités compétentes selon les dispositions légales et réglementaires en vigueur ; elles peuvent également être communiquées à l'Utilisateur, pour les seules données qui le concernent directement et individuellement, en application des dispositions du sous-chapitre 12.1 de la présente charte.

160. Les sauvegardes réalisées par le SDMIS ne concernent pas les éléments personnels (messages et fichiers) et les SMS qui sont sauvegardés sous la seule responsabilité de l'Utilisateur.

Chapitre 16 – Sanctions

161. Chaque Utilisateur est responsable, dans le cadre de son activité professionnelle, de l'utilisation des Ressources informatiques en conformité avec la présente charte.

162. Le non-respect de tout ou partie des règles définies dans la présente charte pourra entraîner pour l'Utilisateur la révision par la Direction du SDMIS des Ressources informatiques mises à disposition et, le cas échéant, des sanctions disciplinaires et/ou des poursuites judiciaires.

MODALITES D'APPLICATION

Chapitre 17 – Entrée en vigueur

163. La présente charte est annexée au Règlement intérieur du SDMIS et publiée sur l'intranet du SDMIS.

GLOSSAIRE

- « **Administrateur** »
 - Désigne toute personne habilitée par le SDMIS aux fins d'assurer le fonctionnement et la sécurité des Ressources informatiques et qui dispose, à ce titre, de droits d'accès privilégiés sur les Ressources informatiques dont il n'est pas l'Utilisateur direct ;
- « **ANSSI** »
 - Agence Nationale de la Sécurité des Systèmes d'Information ;
- « **CGU** »
 - Conditions Générales d'Utilisation ;
- « **Cloud** »
 - « Informatique en nuage ». Désigne l'ensemble des matériels, réseaux et logiciels fournissant des services exploitables via Internet.
- « **CNIL** »
 - Commission Nationale de l'Informatique et des Libertés ;
- « **Donnée à caractère personnel** »
 - Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou tout autre personne (Article 2 de la loi « Informatique et libertés du 6 janvier 1978 ») ;
- « **DPD** »
 - Délégué à la Protection des Données ;
- « **GBAT** »
 - Groupement Bâtiments ;
- « **GSI** »
 - Groupement des Systèmes d'Information ;
- « **Hiérarchie** »
 - Désigne l'autorité hiérarchique directe sous laquelle est placé l'Utilisateur (n+1) ;
- « **Nomades** »
 - Toutes les Ressources informatiques qui peuvent être utilisées par l'Utilisateur dans le cadre de ses déplacements professionnels hors du site du SDMIS (ordinateurs portables, smartphones, tablettes, postes de radio, ...) ;
- « **Ressources informatiques** »
 - Ensemble des moyens informatiques, téléphoniques et de communication électronique du SDMIS. Ils comprennent, de façon non limitative :
 - Les ordinateurs fixes ou portables, smartphones ou tablettes, téléphones fixes ou portables, équipements radio, serveurs, le matériel de visioconférence ainsi que tout autre matériel informatique, connectique ou bureautique ;
 - Les logiciels, progiciels, applications faisant fonctionner, inter-opérer ou protégeant lesdits ordinateurs et matériels ;

- L'ensemble des services de traitement et de stockage d'informations et de communications comprenant notamment la messagerie électronique, l'informatique en nuage (ci-après le « Cloud ») et les accès internet et intranet ;
- L'ensemble des informations stockées sur lesdits ordinateurs et matériels ;
- « **RGPD** »
 - Règlement Général sur la Protection des Données ;
- « **RSSI** »
 - Responsable de la Sécurité des Systèmes d'Information ;
- « **SDMIS** »
 - Service Départemental-Métropolitain d'Incendie et de Secours ;
- « **SI** »
 - Système d'Information. Ensemble organisé de Ressources informatiques permettant de collecter stocker, traiter et distribuer de l'information ;
- « **Traitement de Données à caractère personnel** »
 - Toute opération ou tout ensemble d'opérations portant sur de telles Données, 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 ;
- « **Utilisateur** »
 - Toute personne, tous statuts juridiques confondus, autorisée par le SDMIS à utiliser les Ressources informatiques, de façon permanente ou temporaire ;

Sont notamment considérés comme Utilisateurs au sens de la présente charte :

- L'ensemble des personnels du SDMIS, tels qu'ils sont définis à l'article 1.1. du Règlement intérieur, et ce quel que soit leur statut (agents titulaires et non-titulaires, personnel intérimaire, vacataire, stagiaire, etc.) ;
- Les personnels des prestataires extérieurs (sous relation contractuelle) ;
- Et tous les collaborateurs externes autorisés à accéder au SI du SDMIS ;
- « **VPN** »
 - Réseau Privé Virtuel ou en anglais Virtual Private Network. Système permettant de créer un lien direct et sécurisé entre des ordinateurs distants.

SDMIS
SAPEURS-POMPIERS

**ANNEXE N°1 A LA CHARTE UTILISATEURS–UTILISATION DES
MOYENS INFORMATIQUES, TELEPHONIQUES ET DE
COMMUNICATION ELECTRONIQUE**

CHARTRE
ADMINISTRATEURS
DES SYSTEMES D'INFORMATION

Table des matières

1.	CONTEXTE	3
2.	DEFINITIONS	3
3.	OBJET	3
4.	PREROGATIVES DES ADMINISTRATEURS	4
4.1	ADMINISTRATION DES RESSOURCES INFORMATIQUES.	4
4.1.1.	Transparence des interventions	4
4.1.2.	Gestion et surveillance	4
4.1.3.	Opérations de maintenance et d'audit	4
4.2	GESTION DE LA SECURITE DES RESSOURCES INFORMATIQUES	5
4.2.1	Prérogatives d'ordre général	5
4.2.2	Prérogatives spécifiques en cas d'utilisation de matériels personnels à des fins professionnelles	6
4.2.3	Sauvegarde et maintien des éléments de preuve	6
5.	ENGAGEMENTS DES ADMINISTRATEURS	6
5.1	COLLABORATION ET COOPERATION	7
5.2	CONSEIL ET ALERTE	7
5.3	OBLIGATIONS DE CONFIDENTIALITE ET DE SECURITE RENFORCES	7
5.3.1	Confidentialité	7
5.3.2	Sécurité	8
5.4	RESPECT DE LA PROPRIETE INTELLECTUELLE	8
5.5	RESPECT DE LA VIE PRIVEE	8
5.6	RESPECT DE LA REGLEMENTATION SUR LES DONNEES A CARACTERE PERSONNEL	8
5.7	RESPECT DE LA REGLEMENTATION ET DES NORMES APPLICABLES	9
6.	RESPONSABILITE DES ADMINISTRATEURS	9
7.	EVOLUTION DE LA PRESENTE CHARTE	9

1. CONTEXTE

1. Le SDMIS dispose au sein de son personnel de personnes responsables de son système d'information et de communication, autrement dénommées « Administrateurs ». Sur un périmètre d'intervention défini, ces Administrateurs peuvent être du personnel externe au SDMIS.

2. Les Administrateurs ont pour mission générale la gestion, l'administration et l'exploitation des Ressources informatiques.

3. L'Administrateur assure la gestion :

- Des accès informatiques, de la messagerie électronique, de l'accès à Internet, des listes de diffusions ;
- Des postes informatiques et des serveurs du SDMIS ;
- Des comptes des Utilisateurs, tels que l'ouverture, les droits, la limitation de l'utilisation des ressources réseaux et la clôture après avoir obtenu si nécessaire l'accord de la Hiérarchie ;
- Du réseau informatique, tels que l'installation de point d'accès Wi-Fi, le paramétrage des routeurs, le cloisonnement des usages, le filtrage et le raccordement de nouveaux sites et de nouveaux réseaux ou sous-réseaux ;
- Des applications métiers et techniques du SDMIS ;
- De l'ensemble des données et informations du SDMIS ;
- De tout autre Ressource informatique ;

4. Afin d'être en mesure de remplir leur mission, les Administrateurs disposent de droits étendus quant à l'utilisation et à la gestion des Ressources informatiques.

5. Chaque Administrateur est désigné par le Directeur Départemental et Métropolitain, sur proposition du chef du GSI.

6. A cette fin, il est établi une liste des Administrateurs, indiquant la nature de leur mission ainsi que leur périmètre d'intervention. Cette liste sera mise à jour autant que de besoin.

7. Le SDMIS se réserve la possibilité de retirer à tout moment à l'Administrateur les prérogatives qui lui ont été accordées.

8. L'objectif du présent document (ci-après « la Charte Administrateur ») est d'assurer la pérennité et la sécurité des Ressources informatiques, tout en préservant les droits et libertés fondamentaux des Utilisateurs.

9. La Charte administrateur pourra évoluer en fonction du contexte légal et de la politique de sécurité applicable au sein du SDMIS.

2. DEFINITIONS

10. La Charte Administrateur constitue l'annexe n°1 de la charte d'utilisation des Ressources informatiques du SDMIS (ci-après « la Charte Utilisateurs »).

11. En conséquence, l'ensemble des termes commençant par une majuscule dans la Charte Administrateur a la même signification que ceux définis dans le glossaire de la Charte Utilisateurs.

3. OBJET

12. La Charte Administrateur a pour objet de définir les prérogatives, les engagements et la responsabilité des Administrateurs.

13. Elle complète la Charte Utilisateurs mais ne s'y substitue pas. Elle a pour vocation de délimiter le périmètre d'intervention de l'Administrateur.

4. PREROGATIVES DES ADMINISTRATEURS

4.1 ADMINISTRATION DES RESSOURCES INFORMATIQUES

4.1.1. Transparence des interventions

14. L'Administrateur a le devoir d'informer, dans la mesure du possible, les Utilisateurs de toute intervention susceptible de perturber ou d'interrompre l'utilisation habituelle des Ressources informatiques.

15. L'Administrateur s'engage à ne pas consulter directement ou indirectement de données personnelles d'un Utilisateur, à l'exception de motifs l'y autorisant conformément à l'exercice de ses prérogatives.

16. L'Administrateur ne peut effectuer une « prise de main à distance » qu'après accord préalable de l'Utilisateur sauf en cas de nécessité absolue de sécurité ou d'absence de celui-ci.

17. L'Administrateur s'engage à ne jamais demander le mot de passe à l'Utilisateur.

18. Dans l'hypothèse où lesdites interventions sont imposées par des autorités judiciaires et/ou administratives, l'Administrateur n'a pas à en informer les Utilisateurs.

4.1.2. Gestion et surveillance

19. L'Administrateur assure la gestion des traces, des fichiers de journalisation du SI et des profils des Utilisateurs suivant les conditions prévues dans le registre de traitement de données à caractère personnel.

20. Il donne accès aux applications du SDMIS, selon les règles en vigueur et après avoir obtenu l'accord de la Hiérarchie de l'Utilisateur.

21. L'Administrateur s'engage à ce que l'accès aux Ressources informatiques du SDMIS ne puisse pas se faire par l'intermédiaire de comptes génériques sauf dérogation validée par le RSSI.

22. Dans le cadre de ses fonctions, il veille également au respect, par les Utilisateurs, des dispositions de la Charte Utilisateurs et assure leur sensibilisation sur la sécurité du SI et la protection des données dès que nécessaire.

23. Il pourra, à cette fin, effectuer des opérations de contrôle et de surveillance de l'utilisation des Ressources informatiques, dans les conditions définies dans le chapitre 13 « Mesures de contrôle » de la Charte Utilisateurs.

24. A ce titre, ce chapitre 13 de la Charte Utilisateurs s'applique également aux Administrateurs afin d'assurer une plus grande traçabilité. Le SDMIS se réserve le droit de mettre en œuvre des outils spécifiques à cet usage.

25. Le non-respect des dispositions de la Charte Utilisateurs devra être signalé sans délai par l'Administrateur à sa Hiérarchie.

4.1.3. Opérations de maintenance et d'audit

26. L'Administrateur maintient le bon état de fonctionnement général des Ressources informatiques.

27. Il s'engage à faire ses meilleurs efforts pour assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité du SI du SDMIS.

28. A cette fin, il applique les procédures de maintenance préventive des Ressources informatiques.

29. De plus, l'Administrateur met en œuvre une maintenance curative des Ressources informatiques.

30. Il procède ainsi à la correction des anomalies du SI. Il préconise et met en place des solutions de contournement permettant d'assurer la continuité du service.

31. A ce titre, l'Administrateur utilise tous les moyens de sécurité mis à sa disposition pour procéder à cette maintenance curative et met notamment en place les correctifs de sécurité nécessaires à la maintenance du SI.

32. L'Administrateur pourra, sur demande de sa Hiérarchie, procéder à un audit interne du SI, afin de vérifier l'utilisation des Ressources informatiques, dans un but de maintenance préventive ou curative ou en cas d'urgence.

33. Dans ce cadre, l'Administrateur a toute latitude pour analyser les traces et les historiques permettant de reconstituer l'activité des Utilisateurs selon les finalités prévues dans le registre de traitement de données à caractère personnel.

4.2 GESTION DE LA SECURITE DES RESSOURCES INFORMATIQUES

4.2.1 Prérogatives d'ordre général

34. L'Administrateur participe à la mise en œuvre de la politique de sécurité du SDMIS.

35. Conformément aux directives de sa Hiérarchie et aux procédures mises en place au sein du SDMIS, l'Administrateur doit prendre toutes les mesures nécessaires au maintien d'un niveau de sécurité suffisant des Ressources informatiques dans son périmètre de responsabilité.

36. A cette fin, il assure une surveillance des applications techniques de sécurité mises en place et informe la Hiérarchie des dysfonctionnements techniques constatés et de toutes les anomalies découvertes telles que, notamment, les intrusions dans le réseau et le SI.

37. Pour toute action d'administration, l'Administrateur s'engage à utiliser le compte d'administration à sa disposition ayant les droits d'accès nécessaires et suffisants. Pour toute autre action, il doit utiliser son compte Utilisateur et se conformer à la Charte Utilisateurs associée.

38. A ce titre, l'Administrateur ne doit jamais utiliser un compte d'administration pour se connecter à un poste de travail.

39. A ce titre, l'Administrateur s'engage à accéder à Internet uniquement depuis son compte Utilisateur (sous-chapitre 3.3 de la Charte Utilisateurs).

40. Tout mot de passe utilisé par un Administrateur doit suivre la politique de gestion des mots de passe du SDMIS et être modifié selon une fréquence déterminée par le SDMIS. Un Administrateur s'engage à utiliser un (ou plusieurs) coffre(s)-fort(s) numérique(s) (tel que Keepass) pour gérer l'ensemble des mots de passe d'administration.

41. L'Administrateur devra utiliser les moyens mis à sa disposition par sa Hiérarchie pour empêcher l'activation de virus, de bombes logiques, de chevaux de Troie ou autres logiciels malveillants, provenant notamment de l'ouverture de messages reçus par les systèmes de messagerie ou lors de l'accès à Internet par les Utilisateurs.

42. En cas de doute sur l'efficacité des mesures, l'Administrateur devra appliquer le principe de précaution et détruire les fichiers susceptibles de porter atteinte à la disponibilité, l'intégrité et la confidentialité des Ressources informatiques avec l'accord préalable de sa Hiérarchie.

43. 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 des Ressources informatiques, s'il estime qu'il dispose de la compétence nécessaire ou que les conséquences de son inaction font courir un risque supérieur à celui de son intervention.

44. Dans cette hypothèse, il informe immédiatement sa Hiérarchie des actions qu'il met en œuvre et des solutions alternatives qu'il est amené à adopter.

45. L'Administrateur pourra procéder à une analyse approfondie sur demande de sa Hiérarchie, ou s'il estime que cette analyse est nécessaire pour comprendre le dysfonctionnement et éviter qu'il ne se reproduise.

46. L'Administrateur ne pourra procéder à une modification du mot de passe de l'Utilisateur que sur demande explicite de celui-ci.

47. En cas de violation de la Charte Utilisateurs, l'Administrateur pourra verrouiller les comptes d'accès des Utilisateurs concernés, sous réserve d'en informer immédiatement sa Hiérarchie.

4.2.2 Prérogatives spécifiques en cas d'utilisation de matériels personnels à des fins professionnelles

48. L'Administrateur s'engage à ne connecter aucun matériel personnel sur un équipement d'administration (disque dur, clé USB, téléphone portable, cigarette électronique, cartes SD, ...).

49. L'Administrateur pourra procéder à toute déconnexion de matériel personnel qu'il jugerait nécessaire pour pallier une atteinte à la sécurité ou tout autre risque de toute nature, à tout moment et pour quelque cause que ce soit.

50. En tout état de cause, l'Administrateur pourra s'assurer du respect par chaque Utilisateur concerné des CGU qui seront applicables à l'usage à titre professionnel des Ressources informatiques personnelles, qui sont visées au sous-chapitre 5.6 de la Charte Utilisateurs.

51. En cas de non-respect des dispositions de ces CGU, l'Administrateur s'engage à en informer sans délai sa Hiérarchie, et à suivre ses instructions le cas échéant.

4.2.3 Sauvegarde et maintien des éléments de preuve

52. Les sauvegardes nécessaires de fichiers, de données et de traitements du SDMIS seront effectuées par l'administrateur de manière régulière et conformément aux instructions de la direction du GSI du SDMIS.

53. Lorsqu'un incident de sécurité intervient, l'Administrateur doit agir au plus vite afin de conserver les éléments de preuve, à savoir :

- Déconnecter les Ressources informatiques du réseau afin d'éviter toute action d'effacement ou de modification de preuve postérieure à la découverte de l'incident ;
- Éviter d'éteindre les Ressources informatiques incriminées. Si néanmoins l'extinction est nécessaire, la méthode d'extinction devra préserver autant que possible les preuves liées à l'incident ;
- Éviter de connecter des supports amovibles pour ne pas générer de traces dans la journalisation ;
- Restreindre l'accès physique aux Ressources informatiques incriminées afin de préserver leur intégrité jusqu'à l'intervention des services compétents,
- Verrouiller, si nécessaire, les comptes Utilisateurs ;
- Tracer son intervention ;

54. L'Administrateur doit se conformer à un plan de sauvegarde, qui devra présenter les meilleures garanties de sécurité et garantir la continuité des opérations.

5. ENGAGEMENTS DES ADMINISTRATEURS

55. De façon générale, l'Administrateur s'engage à respecter les dispositions de la Charte Utilisateurs, au même titre que tout Utilisateur.

56. Toutefois, l'Administrateur s'engage, dans le cadre de ses fonctions, à respecter les obligations suivantes :

5.1 COLLABORATION ET COOPERATION

57. L'Administrateur coopère étroitement avec la direction du GSI du SDMIS.

58. A cette fin, il procède à un échange permanent d'informations en vue de contribuer à la bonne exécution de ses obligations et au fonctionnement du SI du SDMIS.

59. A ce titre, l'Administrateur informe sa Hiérarchie de tous les faits constitutifs de délits ou de crimes (notamment les contenus illicites à caractère pédopornographique) dont il pourrait avoir connaissance dans le cadre de ses fonctions.

60. L'Administrateur collabore étroitement avec les autorités compétentes, notamment la CNIL et avec toute autorité judiciaire ou administrative qui pourrait requérir la communication d'information.

5.2 CONSEIL ET ALERTE

61. L'Administrateur a une obligation générale de conseil, d'alerte et de mise en garde auprès de la direction du GSI du SDMIS.

62. Il assure à cette fin une surveillance générale des Ressources informatiques, et informe immédiatement sa Hiérarchie de tout dysfonctionnement qu'il pourrait constater.

5.3 OBLIGATIONS DE CONFIDENTIALITE ET DE SECURITE RENFORCES

5.3.1 Confidentialité

63. L'Administrateur est soumis au secret professionnel et s'engage à respecter une confidentialité absolue sur l'ensemble des données, fichiers, traitements et informations dont il pourrait avoir connaissance dans l'exercice de ses prérogatives.

64. L'Administrateur s'engage à ne pas divulguer à des tiers toutes informations confidentielles ou sensibles pour la sécurité du SI dont il a connaissance sauf sur demande explicite de sa Hiérarchie.

65. L'Administrateur s'engage à utiliser un mot de passe administrateur strictement différent de son mot de passe Utilisateur. Ce mot de passe devra être conforme au sous-chapitre 4.2 « Identifiant et mot de passe personnels » de la Charte Utilisateurs.

66. De plus, il s'engage à garder strictement confidentiel son mot de passe administrateur et à ne le dévoiler à personne, ni l'écrire, ni l'enregistrer sur un support quelconque pour la mémorisation, sauf en cas de nécessité de continuité de service.

67. Dans cette hypothèse, l'Administrateur devra prendre les mesures nécessaires pour protéger le support en question (chiffrement, stockage dans un coffre).

68. En outre, en cas d'externalisation des opérations de maintenance, l'Administrateur :

- S'assure de la cohérence des droits attribués au prestataire avec le périmètre d'intervention et de la traçabilité de leurs interventions.
- S'engage à limiter sa communication au strict nécessaire (partage de données d'architecture / informations techniques en lien direct avec le périmètre d'intervention).
- S'assure que les prestataires n'accèdent qu'aux données informatiques nécessaires à l'accomplissement de leur mission
- S'assure que les prestataires s'engagent par contrat à respecter la confidentialité dont ils auraient eu connaissance au cours de leur prestation.

5.3.2 Sécurité

69. L'Administrateur s'engage à ne pas prendre ses consignes d'une personne non habilitée et à faire remonter auprès de son responsable hiérarchique toute requête lui paraissant inappropriée.

70. L'Administrateur s'engage à n'utiliser que les Ressources informatiques autorisées par sa Hiérarchie, et s'interdit en conséquence d'utiliser tout autre Moyen lors de ses interventions.

71. A ce titre, il devra notamment utiliser les solutions mises à sa disposition pour empêcher l'activation de virus et toute autre tentative d'intrusions externes sur le réseau du SDMIS.

72. Afin d'assurer un niveau de sécurité suffisant, l'Administrateur procède aux mises à jour régulière des logiciels et/ou progiciels du SI avec une attention particulière aux composants de sécurité.

5.4 RESPECT DE LA PROPRIETE INTELLECTUELLE

73. L'Administrateur s'engage à respecter les droits de propriété intellectuelle des tiers, et notamment du SDMIS.

74. A ce titre, il s'engage à ce que :

- Les logiciels et/ou progiciels soient utilisés dans les conditions de licences souscrites par le SDMIS ;
- Les logiciels, bases de données, pages web ou autres créations de tiers protégées par le droit d'auteur, ou un droit privatif ne soient pas reproduits, utilisés ou remis à des tiers ;

75. A ce titre, l'Administrateur devra mettre en place les moyens définis par le SDMIS visant à garantir le respect de ces droits, notamment en cas de téléchargement illicite (filtrage de sites internet, restrictions sur les protocoles, etc.).

5.5 RESPECT DE LA VIE PRIVEE

76. L'Administrateur s'engage à respecter la vie privée des Utilisateurs qui disposent notamment d'un droit à une vie privée résiduelle relatif à l'utilisation des Ressources informatiques, tel que défini au sous-chapitre 6.2 de la Charte Utilisateurs.

77. A ce titre, l'Administrateur qui serait amené, de manière exceptionnelle, dans la limite des possibilités tolérées dans un tel cas, dans le cadre de ses fonctions, à avoir accès aux dossiers, fichiers, données et messages identifiés comme « Privé » ou « Personnel » s'engage à en assurer la confidentialité tout en respectant le sous-chapitre 5.1 « Nomadisme » concernant ses engagements de collaboration et de coopération.

5.6 RESPECT DE LA REGLEMENTATION SUR LES DONNEES A CARACTERE PERSONNEL

78. L'Administrateur s'engage à respecter les dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et à se conformer au RGPD du 14 avril 2016.

79. A ce titre, il informe sans délai le DPD et sa Hiérarchie de tout traitement de données à caractère personnel qu'il serait amené à réaliser dans le cadre de ses fonctions.

80. L'Administrateur collabore avec le DPD pour respecter, le cas échéant, les droits des personnes concernées par ledit traitement, notamment en ce qui concerne leur droit d'accès, de rectification et d'opposition.

81. Dans l'hypothèse d'une étude statistique et lorsque cela s'avère nécessaire pour respecter le RGPD, l'Administrateur doit préalablement anonymiser de manière irréversible les données à caractère personnel. En cas de doute, l'Administrateur contactera le DPD.

82. Il s'engage, en outre, au respect de la sécurité, de la finalité et de la confidentialité des données à caractère personnel figurant dans les fichiers appartenant au SDMIS.

5.7 RESPECT DE LA REGLEMENTATION ET DES NORMES APPLICABLES

83. L'Administrateur s'engage au respect de la réglementation et des normes applicables au SDMIS telles qu'elles lui sont notifiées.

6. RESPONSABILITE DES ADMINISTRATEURS

84. L'Administrateur s'engage à assurer sa mission dans les limites de la Charte Administrateur, de la Charte Utilisateurs, et de son statut.

85. L'Administrateur s'engage à produire toutes les documentations nécessaires à la bonne gestion du SI.

86. L'Administrateur s'applique à documenter ses actions sur le SI tout en assurant la mise à jour des procédures appliquées.

87. Le non-respect de tout ou partie des règles définies dans la présente charte pourra entraîner pour l'Administrateur la suppression immédiate de ses prérogatives et, le cas échéant, des sanctions disciplinaires et/ou des poursuites judiciaires.

7. EVOLUTION DE LA PRESENTE CHARTE

88. Chaque Administrateur est invité à transmettre à la direction du GSI du SDMIS toute proposition de modification ou d'ajout dont il a pu constater l'intérêt dans le cadre de sa mission.

89. La présente charte est publiée sur l'intranet du SDMIS et annexée à la Charte Utilisateurs, elle-même annexée au Règlement intérieur du SDMIS.