N°2018-CA-25

- Membres théoriques : 17
- Membres en exercice : 17
- Membres présents : 11
- Pouvoirs : 2
- Votants : 13

CONSEIL D'ADMINISTRATION DU SERVICE DEPARTEMENTAL D'INCENDIE ET DE SECOURS DE LA SEINE-MARITIME

EXTRAIT DES DELIBERATIONS

EVOLUTIONS DU REGLEMENT INTERIEUR DU SDIS 76

Le 28 juin 2018, le Conseil d'administration du Service départemental d'incendie et de secours de la Seine-Maritime, convoqué le 12 juin 2018, s'est réuni à la direction départementale sous la présidence de Monsieur André GAUTIER.

Le quorum étant atteint (9 membres) avec 11 membres présents, l'assemblée peut valablement délibérer.

Étaient présents : Monsieur André GAUTIER, Président,

I. Membres du Conseil d'administration avec voix délibérative :
Titulaires
Mmes Sophie ALLAIS, Pierrette CANU, Florence DURANDE, Blandine LEFEBVRE.
MM. Bastien CORITON, Gérard JOUAN, Michel LEJEUNE, Didier REGNIER, Sébastien TASSERIE.
Suppléant
M. Eric BLOND.

II. Membres avec voix consultative :
MM. le Colonel hors classe Jean-Yves LAGALLE, Directeur départemental, le Colonel Thierry SENEZ, le Commandant Luc TACONNET, le Commandant Hervé TESNIERE, le Caporal Thomas BRU, Pascal GRESSER, Payeur départemental.

III. Membre de droit :
M. Stéphane JARLÉGAND, Directeur de Cabinet.

IV. Pouvoirs :
Madame Florence THIBAUDEAU RAINOT à Monsieur André GAUTIER,
Monsieur Luc LEMONNIER à Monsieur Sébastien TASSERIE.

Étaient absents excusés :
Mmes Chantal COTTEREAU, Florence THIBAUDEAU RAINOT.
MM. Guillaume COUTEY, Luc LEMONNIER, Philippe LEROY, Jean-Pierre THEVENOT, le Colonel hors classe Marc VITALBO, Directeur départemental adjoint, le Commandant Samuel PERDRIX - représenté, le Lieutenant Hervé PASQUIER.

Délibération affichée le : *et retirée de l'affichage le :*

Délibération insérée au recueil des actes administratifs du mois :

Vu :

- *le code général des collectivités territoriales,*
- *l'arrêté n°2018/GAGAJ-007 du Président du Conseil d'administration en date du 07 avril 2018 portant Règlement intérieur du Service départemental d'incendie et de secours de la Seine-Maritime.*

*
**

I - Ajustement du règlement départemental fixant l'attribution des indemnités allouées aux sapeurs-pompiers volontaires (ANNEXE 13)

Le règlement départemental fixant l'attribution des indemnités allouées aux sapeurs-pompiers volontaires adopté au conseil d'administration du 13 décembre 2017 annexé au règlement intérieur est appliqué depuis le 1er janvier 2018.

Pour mémoire, ce règlement fixe le cadre et les modalités d'attribution des indemnités versées aux sapeurs-pompiers volontaires dans les activités qu'ils sont amenés à exercer dans les domaines suivants :

- opérationnel,
- formation,
- encadrement,
- fonctionnement des centres,
- service de santé et de secours médical,
- dispositifs particuliers (groupes de travail, chargé de mission, surveillance des plages,…).

Aussi, conformément au principe édicté, ce règlement fait l'objet d'un suivi permanent permettant de recenser les difficultés rencontrées dans sa mise en œuvre, d'y apporter les compléments d'information nécessaires auprès des différents acteurs, de corriger au besoin le paramétrage des outils de gestion et d'identifier les manques de réponse sur certaines thématiques.
Un premier bilan de suivi permet de vous proposer les premiers ajustements prioritaires dans l'attente d'une évaluation plus globale en fin d'année à savoir :

- ajustement temporaire de l'enveloppe de fonctionnement sur les Cis Aumale et Forges-les-Eaux. En effet, ces deux Cis conformément au règlement ne sont pas éligibles à indemnisation au regard du fait qu'ils disposent normalement d'un effectif de garde de trois sapeurs-pompiers en jour semaine.
  Aussi faute de tenir cet EOJ, la réalisation de certaines tâches est assurée par des effectifs hors garde. Afin de pallier le déficit d'EOJ de garde en jour-semaine, accorder une augmentation de l'enveloppe de fonctionnement au prorata du taux d'atteinte de l'EOJ soit plus 80 %.

- mise en place d'une enveloppe forfaitaire d'heures « présence au Cis » par Cis d'un volume annuel d'heures estimé à 12 heures permettant d'indemniser un sapeur-pompier dont la présence au Cis est rendue nécessaire par l'intervention au sein du Cis d'une prestation interne ou par une entreprise extérieure,

- attribution à chaque groupement Territorial d'une enveloppe d'heures (600 heures) et d'une enveloppe également de 600 heures à disposition de l'ensemble des groupements fonctionnels permettant de répondre à des demandes ponctuelles.

Ces ajustements ont aussi vocation à apporter de la souplesse au dispositif, de répondre aux attentes du terrain tout en maîtrisant l'impact financier.

*

* *

II – Insertion d'un nouveau titre 2 « Dispositions générales » et deux annexes

Au travers de la loi n°2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires, le législateur a souhaité rappeler de manière explicite les valeurs déontologiques communes de la fonction publique en complétant notamment à cet effet la loi du 13 juillet 1983.
En effet, le législateur a entendu définir la déontologie des fonctionnaires comme l'ensemble des règles qui regroupe et régit le comportement des agents publics et permet de définir collectivement la façon d'agir pour servir l'intérêt général.

De plus, récemment l'État a entendu mettre en avant la lutte contre les violences sexuelles et sexistes dans la fonction publique (*Circulaire du 09 mars 2018 – NOR : CPAF1805157C*). Le Sdis 76, en sa qualité d'employeur public, entend se montrer exemplaire dans la prévention et la lutte contre ces violences et contre toutes formes de violences à l'égard de ses agents.

Une démarche plus large sera entamée avec l'ensemble des parties prenantes de l'établissement pour la mise en œuvre des prescriptions présentées par la circulaire sus évoquée (*recensement des violences, mise en place d'un circuit de signalement et d'accompagnement…*).

Enfin, le règlement (européen) général de protection des données (RGPD) impose notamment aux collectivités territoriales et établissements publics d'assurer la sécurité des traitements et des données à caractère personnel et ce à compter du 25 mai 2018. Le Sdis 76 est actuellement en train de se préparer à cette échéance avec la participation du Département.

Cependant, il appartient au service d'assurer la sécurité de ses installations et de ses ressources dont les systèmes d'information et de communication (SIC). Afin de répondre à ce premier défi, il appartient à tous les agents d'être contributeurs et de faire un bon usage des moyens et ressources qui peuvent être mis à disposition.

*

**

Ainsi et pour prendre en compte les principes et les prescriptions précédemment évoqués, il vous est proposé d'intégrer au Règlement intérieur du Sdis 76, un nouveau titre 2 « Dispositions générales ».

Dans un 1er chapitre, seront intégrés les principes déontologiques mais également la question de la lutte contre les violences dont les agents peuvent être victimes avec l'intégration du guide de protection fonctionnelle **en annexe 14**.

Dans un 2nd chapitre, seront intégrées les dispositions relatives à la communication et à l'usage des systèmes d'information et de communication. Ces dispositions conduisent à l'intégration d'un nouveau document structurant qu'est la Charte de sécurité informatique et du bon usage des ressources informatiques et numériques **en annexe 15**.

Cette charte a pour finalité de définir les règles d'utilisation et de préciser les responsabilités des utilisateurs et des administrateurs conformément à la législation en vigueur, et de permettre ainsi un usage normal, optimal et sécurisé des ressources informatiques et téléphoniques mises à disposition des agents du Sdis 76.

Dans un 3ème chapitre, aux fins de cohérence du règlement intérieur, il vous est proposé d'intégrer les dispositions relatives aux matériels et véhicules précédemment traité dans l'ancien titre 7. Il vous est également proposé de supprimer l'alinéa 2 relatif au guidage des conducteurs lors de manœuvres de véhicules opérationnels porté à l'article 2302-2, qui n'a pas de lien direct avec les mentions précédentes dudit article. Ces éléments pourront être repris dans le cadre des réflexions et travaux menés au titre de la filière conduite.

*
**

Enfin, d'autres modifications interviennent pour prendre en compte des correctifs.

Tout d'abord, en lien avec la modification de l'article anciennement 3300-9 du règlement intérieur présenté approuvée par le Conseil d'administration du 04 avril 2018, il vous est proposé de supprimer dans l'article 5200-5 (nouvelle numérotation), la mention relative aux onze heures de repos de sécurité précédent les périodes travaillées. En effet, aucune disposition du décret **n°2001-1382 du 31 décembre 2001 relatif au temps de travail des sapeurs-pompiers professionnels n'impose un repos de sécurité précédent les périodes travaillées.**

« *Après examen des demandes exprimées par les agents, le chef de centre arrête :*
le planning prévisionnel, un mois au moins avant le début du cycle annuel,
le planning ajusté, sept jours ouvrés avant le début du mois.
Le planning comporte l'ensemble des activités de service connues, les congés annuels et les périodes d'absence. Les périodes de garde se répartissent de manière équilibrée sur les deux semestres du cycle annuel.
~~*Le repos de sécurité précédent les périodes travaillées doit être d'au moins onze heures.*~~ *Le repos de sécurité suivant les périodes travaillées doit être d'une durée au moins égale à celle-ci.*
Chaque agent étant responsable de sa propre sécurité avant chaque prise de garde, il doit respecter une interruption de service lui permettant de prendre sa garde et d'assurer ses missions en toute sécurité.»

*
**

Pour conclure, il vous est proposé :

- une modification dans l'annexe 4 « Congés exceptionnels et autorisations exceptionnelles d'absence applicable aux SPP SHR et PATS » par la suppression d'une mention relevant de l'annexe 4 Bis,
- une modification de l'annexe 9 « liste des agents bénéficiant à titre individuel de la reprise de leurs régimes de garde 12 heures tel qu'au 31 décembre 2013 » pour mise à jour,

- la modification de l'annexe référencée à l'article 5200-13 (l'annexe 8 au lieu de l'annexe 9).

*
**

Conformément aux dispositions du code général des collectivités territoriales, les avis suivants ont été recueillis :

- le comité technique du Sdis a émis lors de sa séance du 14 juin 2018 les avis suivants :
  - pour le collège des représentants de l'administration un avis favorable à l'unanimité sur la proposition d'amendement au rapport ainsi que sur le rapport amendé,
  - pour le collège des représentants du personnel a émis un avis favorable à l'unanimité sur la proposition d'amendement au rapport ainsi que sur le rapport amendé,
- le comité consultatif départemental des sapeurs-pompiers volontaires a rendu un avis favorable à l'unanimité sur le rapport amendé lors de sa séance du 14 juin 2018,
- la commission administrative et technique des services d'incendie et de secours a rendu un avis favorable à l'unanimité lors de sa séance du 25 juin 2018.

*
* *

Après en avoir délibéré, les membres du Conseil d'administration adoptent à l'unanimité ce dossier.

Le président du conseil d'administration,

André GAUTIER

Sapeurs-Pompiers
de Seine-Maritime

SDIS76

Projet

Règlement intérieur

TYPE de Document
Règlement intérieur
MAJ
07/04/2018

anciennes références		nouvelles références	
TITRE 1 ORGANISATION DE L'ETABLISSEMENT PUBLIC *art 1100 à 1500*	P 4-6	TITRE 1 ORGANISATION DE L'ETABLISSEMENT PUBLIC *art 1100 à 1500*	P 4-5
		TITRE 2 DISPOSITIONS GENERALES *art 2100-1 à 2200-6*	P 6-18
TITRE 2 DISPOSITIONS COMMUNES AUX SAPEURS-POMPIERS ET AUX AGENTS RELEVANT DES AUTRES FILIERES *art 2100-1 à 2700-3*	P 6-16	TITRE 3 DISPOSITIONS COMMUNES AUX SAPEURS-POMPIERS ET AUX AGENTS RELEVANT DES AUTRES FILIERES *art 3100-1 à 3600-3*	P 19-28
TITRE 3 DISPOSITIONS COMMUNES A L'ENSEMBLE DES SAPEURS-POMPIERS *art 3100-1 à 3300-19*	P 17-23	TITRE 4 DISPOSITIONS COMMUNES A L'ENSEMBLE DES SAPEURS-POMPIERS *art 4100-1 à 4300-19*	P 29-36
TITRE 4 DISPOSITIONS PROPRES AUX SAPEURS-POMPIERS PROFESSIONNELS *art 4100-1 à 4400-4*	P 24-37	TITRE 5 DISPOSITIONS PROPRES AUX SAPEURS-POMPIERS PROFESSIONNELS *art 5100-1 à 5400-4*	P 37-49
TITRE 5 DISPOSITIONS PROPRES AUX SAPEURS-POMPIERS VOLONTAIRES *art 5100-1 à 5400-6*	P 38-4[illegible]	TITRE 6 DISPOSITIONS PROPRES AUX SAPEURS-POMPIERS VOLONTAIRES *art 6100-1 à 6400-6*	P 50-55
TITRE 6 DISPOSITIONS PROPRES AUX AGENTS NE RELEVANT PAS DE LA FILIERE DES SAPEURS-POMPIERS PROFESSIONNELS *art 6110-1 à 6350-1*	P 43-[illegible]	TITRE 7 DISPOSITIONS PROPRES AUX AGENTS NE RELEVANT PAS DE LA FILIERE DES SAPEURS-POMPIERS PROFESSIONNELS *art 7110-1 à 7350-1*	P 56-64
TITRE 7 AFFECTATION DE VEHICULES DE FONCTION ET UTLISATION DES VEHICULES DE SERVICE *art 7100-1 à 7200-2*	P 52-54	CHAPITRE 3 - TITRE 2 DISPOSITIONS GENERALES *art 2302-1 à 3202-14*	P 14-18
TITRE 8 DISPOSITIONS DIVERSES - CHAPITRE 1 DISPOSITIONS RELATIVES AUX MATERIELS ET INFRASTRUCTURES *art 8100-1 à 8100-3*	P 55-56	CHAPITRE 3 - TITRE 2 DISPOSITIONS GENERALES *art 2301-1à 2301-3*	P 14-18
TITRE 8 DISPOSITIONS DIVERSES - CHAPITRE 2 AUTRES DISPOSITIONS *art 8200-1 à 8200-3*		TITRE 8 DISPOSITIONS DIVERSES *art 8200-1 à 8200-3*	P 65-66

TITRE 2 : Dispositions générales

L'ensemble de ces dispositions est applicable à tous les agents et collaborateurs du Sdis 76 (*fonctionnaires titulaires ou contractuels de toutes les filières, sapeurs-pompiers volontaires et autres collaborateurs du service public*).

Chapitre 1 – Déontologie (droits et obligations)

Article 2100-1

Tous les agents du Sdis 76, fonctionnaires ou non, sont tenus d'exercer leurs missions dans l'objectif de servir l'intérêt général. Ce dernier intègre les principes et les valeurs déontologiques suivants et rappelés par la loi n°2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires :

- *Dignité,*
- *Impartialité,*
- *Intégrité,*
- *Probité,*
- *Neutralité,*
- *Laïcité.*

L'activité quotidienne du Sdis 76 et des agents et collaborateurs qui le composent se traduit au travers de trois valeurs cardinales :

Le respect de l'usager

- ***Obligation d'impartialité***
- ***Obligation de neutralité***
- ***Obligation de secret professionnel***

L'exemplarité

- ***Obligation de probité***
- ***Obligation de dignité dans la vie personnelle***

La loyauté vis-à-vis de l'institution

- ***Obligation de respect du droit applicable***
- ***Obligation de l'exercice exclusif des fonctions***
- ***Obligation d'obéissance***
- ***Obligation de discrétion professionnelle***
- ***Obligation de réserve***

Section 1 : Droits

Article 2100-2

La liberté d'opinion est garantie aux personnels du Sdis *(agents publics et sapeurs-pompiers volontaires)*.
Aucune distinction, directe ou indirecte, ne peut être faite entre les agents en raison de leurs opinions politiques, syndicales, philosophiques ou religieuses, de leur origine, de leur orientation ou identité sexuelle, de leur âge, de leur patronyme, de leur situation de famille, de leur état de santé, de leur apparence physique, de leur handicap ou de leur appartenance ou de leur non-appartenance, vraie ou supposée, à une ethnie ou une race.

Article 2100-3

~~L'exercice du droit syndical est reconnu. Il s'exerce dans le cadre des dispositions statutaires et des notes de service ou circulaires, sous réserve des nécessités et de la continuité du service public. Les modalités d'exercice du droit syndical font l'objet d'un protocole d'accord signé avec les organisations syndicales représentatives.~~

L'exercice du droit syndical s'exerce dans le respect des dispositions législatives et réglementaires relatives à l'exercice de ce droit dans la fonction publique.
Il fait l'objet d'un protocole d'accord.

Le droit de grève est un des droits fondamentaux dont bénéficient notamment les fonctionnaires et les agents non titulaires de la fonction publique. Il est donc reconnu aux agents publics, qui doivent l'exercer dans le cadre des lois qui le réglementent.

Le droit de grève doit pouvoir être exercé tout en assurant le minimum de continuité des services publics dont le Sdis est chargé.
Ainsi, par arrêté conjoint de la Préfète et du Président du Conseil d'administration en date du 07 juin 2016 portant instauration d'un service minimum, le Sdis peut assurer la continuité du service sans porter atteinte au droit de grève. Cet arrêté permet donc au service de concilier le droit des agents à faire grève et la nécessaire continuité de service auprès des seino-marins. Les règles relevant du service minimum sont mentionnées dans l'arrêté susmentionné et accessible sur l'intranet du Sdis 76.

Article 2100-4

Le droit de retrait est une mesure exceptionnelle permettant à un agent public de se retirer d'une situation de travail dont il a un motif raisonnable de penser qu'elle présente un danger grave et imminent pour sa vie ou sa santé.

En application des dispositions de l'article 5-1 du décret n°85-603 du 10 juin 1985, précisées par arrêté du 15 ~~mai~~ mars 2001, pour les sapeurs-pompiers professionnels, le droit de « se retirer » ne peut être mis en avant, dans le cadre des missions de secours, que dans la mesure où l'intégrité physique d'autrui n'est pas menacée du fait de son retrait.
Les mêmes règles doivent être respectées par les sapeurs-pompiers volontaires et les agents publics non titulaires au sens de l'article 3 de la loi n°84-53 du 26 janvier 1984.

Article 2100-5

Aucun agent ne doit subir des faits relevant de la qualification de violence ou de harcèlement, qu'il soit harcèlement moral et/ou harcèlement sexuel. Le Sdis 76, lorsque de tels faits lui seront portés à connaissance, fera cesser les situations de violences en prenant toute mesure conservatoire y compris l'éloignement de l'auteur supposé des faits ou de la victime sans préjuger des enquêtes diligentées et des suites pénales et disciplinaires qui surviendront.

De plus, le Sdis 76 entend se montrer exemplaire en sa qualité d'employeur public pour prévenir autant que possible et faire cesser les faits de violences morales et/ou sexuelles et sexistes commis à l'égard de ses personnels.

- **Violence morale et faits de harcèlement moral**

Conformément à l'article 6 quinquies de la loi n°83-634 du 13 juillet 1983, aucun fonctionnaire ne doit subir les agissements répétés de harcèlement moral qui ont pour objet ou effet une dégradation des conditions de travail susceptibles de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale, ou de compromettre son avenir professionnel.
Les mêmes règles doivent être respectées par les sapeurs-pompiers volontaires et les agents publics non titulaires au sens de l'article 3 de la loi n°84-53 du 26 janvier 1984.

- **Violence sexuelle et sexiste et faits de harcèlement sexuel**

Conformément à l'article 6 ter de la loi n°83-634 du 13 juillet 1983, aucune mesure concernant notamment le recrutement, la titularisation, la formation, la notation, l'évaluation, la promotion, l'affectation et la mutation ne peut être prise à l'égard d'un fonctionnaire en prenant en considération le fait qu'il a subi ou refusé de subir les agissements de harcèlement de toute personne dont le but est d'obtenir des faveurs de nature sexuelle à son profit ou à celui d'un tiers, qu'il a engagé un recours auprès d'un supérieur ou une action en justice visant à faire cesser ces agissements, ou qu'il a témoigné de tels agissements.

Article 2100-6

A raison de ses fonctions et indépendamment des règles fixées par le code pénal et par les lois spéciales, les agents du Sdis (*agent public et sapeur-pompier volontaire*) ou, le cas échéant, les anciens personnels bénéficient d'une protection organisée par l'établissement public qui les emploie à la date des faits en cause ou des faits ayant été imputés de façon diffamatoire.

Lorsqu'un agent du Sdis a été poursuivi par un tiers pour faute de service, l'établissement public doit, dans la mesure où une faute personnelle détachable de l'exercice de ses fonctions n'est pas imputable à l'agent, le couvrir des condamnations civiles prononcées contre lui.

Lorsqu'un agent du Sdis fait l'objet de poursuites pénales à raison de faits qui n'ont pas le caractère d'une faute personnelle détachable de l'exercice de ses fonctions, l'établissement public doit lui accorder sa protection. L'agent entendu en qualité de témoin assisté pour de tels faits bénéficie de cette protection. L'établissement public est également tenu de protéger l'agent qui, à raison de tels faits, est placé en garde à vue ou se voit proposer une mesure de composition pénale.

L'établissement public est tenu de protéger ses personnels contre les atteintes volontaires à l'intégrité de la personne, les violences, les agissements constitutifs de harcèlement, les menaces, les injures, les diffamations ou les outrages dont ils pourraient être victimes sans qu'une faute personnelle puisse leur être imputée. Il est tenu de réparer, le cas échéant, le préjudice qui en est résulté.

La protection peut être accordée, sur leur demande, au conjoint, au concubin, au partenaire lié par un pacte civil de solidarité à l'agent, à ses enfants et à ses ascendants directs pour les instances civiles ou pénales qu'ils engagent contre les auteurs d'atteintes volontaires à l'intégrité de la personne dont ils sont eux-mêmes victimes du fait des fonctions exercées par l'agent.
Le Sdis 76 accompagne de manière privilégiée ses agents. Cet accompagnement se traduit au travers des procédures mises en place et présentées dans le guide de la protection fonctionnelle en annexe 14.

Article 2100-7

Tout agent du Sdis consacre l'intégralité de son activité professionnelle aux tâches qui lui sont confiées. Il ne peut exercer à titre professionnel une activité privée lucrative de quelque nature que ce soit. Cependant des dérogations à ce principe existent et sont développées dans le présent règlement aux articles 3600-1 et suivants.

Section 2 : Obligations

Obligation de réserve :
Tout agent public doit faire preuve de réserve et de mesure dans l'expression écrite et orale de ses opinions personnelles. En effet, le principe de neutralité du service public interdit au fonctionnaire de faire de sa fonction l'instrument d'une propagande quelconque. La portée de cette obligation est appréciée au cas par cas par l'autorité hiérarchique sous contrôle du juge administratif.

Cette obligation ne concerne pas le contenu des opinions (*la liberté d'opinion est reconnue aux agents publics*), mais leur mode d'expression. L'obligation de réserve s'applique pendant et hors du temps de service.

L'obligation de réserve est une construction jurisprudentielle complexe qui varie d'intensité en fonction de critères :

- *la place dans la hiérarchie, l'expression des hauts fonctionnaires étant jugée plus sévèrement,*
- *les circonstances dans lesquelles un agent s'est exprimé, un responsable syndical agissant dans le cadre de son mandat bénéficie de plus de liberté,*
- *la publicité donnée aux propos. si l'agent s'exprime dans un journal local ou dans un important média national,*
- *et les formes de l'expression, si l'agent a utilisé ou non des termes injurieux ou outranciers.*

Cette obligation impose aussi aux agents publics d'éviter en toutes circonstances les comportements susceptibles de porter atteinte à la considération du service public par les usagers. Cette obligation continue de s'appliquer aux agents suspendus de leurs fonctions et en disponibilité.

Discrétion professionnelle : ***article 26 de la loi n°83-634 du 13 juillet 1983***
Un agent public ne doit pas divulguer les informations relatives au fonctionnement de son administration. L'obligation de discrétion concerne tous les documents non communicables aux usagers.
Elle est particulièrement forte pour certaines catégories d'agents : *les militaires ou les magistrats par exemple.*
Cette obligation s'applique à l'égard des administrés mais aussi entre agents publics, à l'égard de collègues qui n'ont pas, du fait de leurs fonctions, à connaître les informations en cause.
Cette obligation peut être levée par décision expresse de l'autorité hiérarchique.

Secret professionnel : ***article 26 de la loi n°83-634 du 13 juillet 1983***
Un agent public ne doit pas divulguer les informations personnelles dont il a connaissance.
Cette obligation s'applique aux informations relatives à la santé, au comportement, à la situation familiale d'une personne, etc.(ex : *informations obtenues dans le cadre du bilan fait sur une victime, informations obtenues lors d'une intervention et relative au cadre familial de la victime …*)
Le secret professionnel peut être levé sur autorisation de la personne concernée par l'information.
La levée du secret professionnel est obligatoire pour assurer :

- *la protection des personnes (révélation de maltraitances, par exemple),*
- *la préservation de la santé publique (révélation de maladies nécessitant une surveillance, par exemple),*
- *la préservation de l'ordre public (dénonciation de crimes ou de délits) et le bon déroulement des procédures de justice (témoignages en justice, par exemple).*

En outre, les administrations doivent répondre aux demandes d'information de l'administration fiscale.
La révélation de secrets professionnels en dehors des cas autorisés est punie d'un an d'emprisonnement et de 15 000 € d'amende

Article 2100-8

La liberté d'expression est reconnue par la Déclaration universelle des droits de l'homme de 1948 ; cependant, elle doit s'exercer dans les limites définies par les lois et règlements. Les domaines concernés sont notamment ceux liés aux opinions politiques, religieuses et philosophiques.
Toutefois, les agents du Sdis sont astreints à une obligation de réserve. Ils doivent, en effet, faire preuve de mesure dans l'expression écrite et orale de leurs opinions personnelles à l'égard des administrés et des autres agents. Cette obligation ne concerne pas le contenu des opinions mais leur mode d'expression.

De plus, les agents du Sdis doivent respecter le principe de laïcité et l'obligation de neutralité du service public en application duquel tous les usagers doivent être traités de façon égale. Ainsi, ils ne doivent pas porter atteinte à la neutralité du service public et au lien de confiance entre les administrés et le service public.

De plus, tous les agents sont tenus au secret professionnel dans le respect des dispositions du code pénal *(article 226-13 du code pénal : la divulgation est punie d'un an d'emprisonnement et de 15000 euros d'amende).*

Ils doivent également faire preuve de discrétion professionnelle pour tous les faits, informations et documents dont ils ont connaissance dans l'exercice ou l'occasion de l'exercice de leurs fonctions.
En dehors des cas expressément prévus par la règlementation, les agents ne peuvent être déliés de cette obligation de discrétion que par décision de justice ou sur une décision expresse de sa hiérarchie.

Enfin, les propos tenus sur internet et notamment sur les réseaux sociaux étant susceptibles d'être qualifiés de propos publics, les agents doivent s'assurer de ne pas contrevenir à l'ensemble de ses devoirs dans le cadre de leur utilisation.

Article 2100-9

Tout agent du Sdis doit faire preuve de respect à l'égard de ses supérieurs hiérarchiques, de ses collègues ainsi que de ses subordonnés et doit adopter un comportement irréprochable et exemplaire à l'égard des autorités et des usagers.

Il doit se conformer aux ~~ordres et~~ instructions de son supérieur hiérarchique, sauf si ces ~~ordres~~ instructions sont à la fois manifestement illégales et de nature à compromettre gravement un intérêt public.

Enfin, tout agent, quel que soit son rang dans la hiérarchie, est responsable de l'exécution des tâches qui lui sont confiées. Il n'est dégagé d'aucune des responsabilités qui lui incombent par la responsabilité propre de ses subordonnés. Il doit rendre compte à sa hiérarchie des missions effectuées et des éventuelles difficultés rencontrées dans l'exécution de celles-ci.

Article 2100-10

Tout agent du Sdis doit, sans délai, informer l'autorité territoriale d'emploi de toute modification de sa situation personnelle susceptible d'avoir des incidences sur le bon fonctionnement du service. (*suspension de permis, modification du casier judiciaire, etc.*).

À noter que perdent la qualité de fonctionnaire, les agents

- *déchus de leurs droits civiques,*
- *dont les mentions portées au bulletin n°2 du casier judiciaire sont incompatibles avec l'exercice des fonctions,*
- *ayant perdu la nationalité française,*
- *étant interdit par décision de justice d'exercer un emploi public,*

- *n'ayant pas réintégré leurs fonctions à l'issue d'une période de disponibilité.*

Article 2100-11

Aucune rémunération directe de la part de l'usager en contrepartie du service rendu n'est admise. Aucun agent du Sdis ne doit ni solliciter ni accepter de cadeaux, faveurs, invitations ou tout autre avantage lui étant destinés, destinés à sa famille ou à ses proches, qui peuvent influer ou paraître influer sur l'impartialité avec laquelle il exerce ses fonctions ou peuvent constituer ou paraître constituer une récompense en rapport avec ses fonctions.

Les agents du Sdis doivent tout mettre en œuvre pour empêcher que leurs intérêts privés entrent en conflit avec leurs fonctions. Il est de leurs responsabilités d'éviter de tels conflits, qu'ils soient réels, potentiels ou susceptibles d'apparaître comme tels.

Étant donné que les agents sont généralement seuls à savoir s'ils se trouvent dans cette situation, ils sont personnellement tenus :

- *d'être attentifs à tout conflit d'intérêt réel ou potentiel ;*
- *de prendre des mesures pour éviter un tel conflit ;*
- *d'informer leur supérieur hiérarchique de tout conflit d'intérêt dès qu'ils en ont connaissance ;*
- *de se conformer à toute décision finale lui enjoignant de se retirer de la situation dans laquelle ils se trouvent ou de renoncer à l'avantage à l'origine du conflit.*

Constitue un conflit d'intérêt toute situation d'interférence entre un intérêt public et des intérêts publics ou privés qui est de nature à influencer ou paraître influencer l'exercice indépendant, impartial et objectif de ses fonctions.

Chapitre 2 – La communication et l'usage des SIC

Section 1 : La communication

Article 2200-1

La communication institutionnelle est gérée par la direction générale et recouvre deux dimensions :

- *la communication interne circulant à l'intérieur de l'établissement,*
- *la communication externe constituée de l'ensemble des moyens de diffusion de l'information à l'extérieur de l'établissement.*

Tout agent amené à communiquer, dans l'exercice de ses fonctions, se doit de :

- *veiller aux obligations de discrétion et de réserve professionnelles,*
- *préserver l'image de l'établissement : toute information ou document diffusé à une ou plusieurs personnes extérieures au Sdis 76 ne doit pas porter atteinte à son image. Les documents doivent respecter la charte graphique et le guide de la rédaction administrative de l'établissement,*
- *assurer une communication interne préalable à toute communication externe : toute diffusion d'images, de sons, de vidéos ou d'écrits produits doit suivre une procédure d'information préalable ou de validation par la voie hiérarchique,*
- *respecter le droit de la propriété intellectuelle et le droit à l'image.*

Article 2200-2

S'agissant des images représentant des agents ou des matériels du Sdis 76, leur utilisation sur des sites internet ou des blogs personnels, ainsi que pour la conception des calendriers ou brochures des amicales, doit faire l'objet d'une autorisation préalable du service de la communication.
De même, toute diffusion de l'image d'un agent, hors les situations opérationnelles*, doit faire l'objet de l'accord préalable de celui-ci.
** utilisations des photos à des seules fins opérationnelles (usage de photos au CTA CODIS pour le dimensionnement d'une intervention...)*

Article 2200-3

La communication opérationnelle comprend toute diffusion d'information ou image relative à une intervention ou mise en situation opérationnelle auprès de personnes extérieures au service.
Les relations avec les médias sont gérées à la direction départementale par :

- le CTA-CODIS en lien avec le service communication et la direction générale,
- l'autorité préfectorale en situation de crise.

Sur intervention, la communication opérationnelle est réalisée sous l'autorité du commandant des opérations de secours (COS) et doit respecter les règles évoquées à l'article 2200-1.

Section 2 : L'utilisation des systèmes d'information et de communication (SIC)

Article 2200-4

Sont considérés comme SIC les :

- *services et logiciels : internet, télécommunications, progiciels et solutions informatiques diverses,*
- *matériels : informatiques (PC fixes, ordinateurs portables, smartphones, tablettes), téléphoniques (fixes ou portables) et reprographiques.*

Article 2200-5

Les SIC sont réservés à un usage professionnel.
Cependant, il peut être toléré que l'utilisation des SIC se fasse à des fins non professionnelles.

Cela doit être exceptionnel, demeurer raisonnable et ne doit pas :
- perturber le bon fonctionnement des SIC, du service et du Sdis 76 en général,
- poursuivre un but lucratif ou même ludique,
- porter atteinte au Sdis ou être susceptible d'engager sa responsabilité.

L'usage, à des fins personnelles et sur le temps de travail, des moyens de communication ne doit pas venir perturber le fonctionnement du service.

Article 2200-6

Les règles d'utilisation des moyens informatiques et de communication du Sdis 76 ainsi que les règles relatives à l'administration desdits moyens sont précisées par la Charte de sécurité informatique et du bon usage des ressources informatiques et numériques arrêtée par le Président du Conseil d'administration et intégrée au présent règlement en annexe 15.

Conformément aux dispositions légales, cette charte est consultable par tous les agents sur le site intranet du Sdis 76.

Chapitre 3 – Dispositions relatives aux matériels et aux véhicules (extrait)

Section 1 : Dispositions relatives aux matériels et aux infrastructures

Section 2 : Dispositions relatives aux véhicules

Sous-section 1 : Les conditions d'utilisation des véhicules de service

Article 2302-2

Quelle que soit la nature du déplacement, les conducteurs des véhicules de service respectent le code de la route et restent maîtres du véhicule dans toutes les circonstances. Un mémento du conducteur précise toutes les consignes à respecter.

~~Les chefs d'agrès guident ou font guider les véhicules lors de toute manœuvre, en mission ou dans l'enceinte du centre de secours.~~

*

**

TITRE 5 : Dispositions propres aux sapeurs-pompiers professionnels

Chapitre 2 – Modalités de gestion du temps de travail des sapeurs-pompiers professionnels en équipe de garde (extrait)

Article 5200-5

Après examen des demandes exprimées par les agents, le chef de centre arrête :

- le planning prévisionnel, un mois au moins avant le début du cycle annuel,
- le planning ajusté, sept jours ouvrés avant le début du mois.

Le planning comporte l'ensemble des activités de service connues, les congés annuels et les périodes d'absence. Les périodes de garde se répartissent de manière équilibrée sur les deux semestres du cycle annuel.

~~Le repos de sécurité précédent les périodes travaillées doit être d'au moins onze heures.~~ Le repos de sécurité suivant les périodes travaillées doit être d'une durée au moins égale à celle-ci.

Chaque agent étant responsable de sa propre sécurité avant chaque prise de garde, il doit respecter une interruption de service lui permettant de prendre sa garde et d'assurer ses missions en toute sécurité.

Article 5200-13

La liste des personnels bénéficiant à titre individuel de la reprise de leur régime de garde douze heures tel qu'au 31 décembre 2013 est jointe en annexe n°~~8~~ 9 au présent règlement et révisée annuellement.

ANNEXES

ANNEXE 4 – Congés exceptionnels et autorisations exceptionnelles d'absence applicables aux SPP SHR et PATS

CONGÉS EXCEPTIONNELS

MOTIF	DURÉE MAXIMUM (en jours)	JUSTIFICATIF À FOURNIR	OBSERVATIONS
A - Naissance ou adoption d'un enfant	3 jours consécutifs inclus dans une période de 15 jours entourant la date de naissance	Extrait de l'acte	
B - Congé de paternité	11 jours consécutifs pour le père dans un délai de 4 mois après la naissance de l'enfant (18 jours en cas de naissances multiples)	Lettre de demande en recommandé avec AR au moins 1 mois à l'avance + Copie du livret de famille	~~Pour les SPP en garde de 24h, ce congé de 11 jours consécutifs représente une exonération de 4 gardes consécutives.~~ ~~Pour les SPP en garde de 12h, il représente une exonération de 5 gardes consécutives.~~
C – Mariage - de l'agent	5 jours ouvrables consécutifs dont le jour de la cérémonie	Extrait de l'acte	
- de l'enfant	3 jours ouvrables consécutifs dont le jour de la cérémonie	Extrait de l'acte	
- des père, mère, belle-mère, beau-père	2 jours ouvrables consécutifs dont le jour de la cérémonie	Extrait de l'acte	
- des autres ascendants ou descendants, des collatéraux du 2nd degré (frères, sœurs, beaux-frères, belles-sœurs)	2 jours ouvrables consécutifs dont le jour de la cérémonie	Extrait de l'acte	
D - PACS - conclusion d'un PACS	5 jours ouvrables consécutifs dont le jour du pacte	Extrait de l'acte	Il ne peut être cumulé des autorisations d'absence pour PACS et pour mariage avec le même conjoint.

E - Décès - du conjoint, concubin, du partenaire d'un PACS, père, mère, enfants et beaux-parents	5 jours ouvrables consécutifs dont le jour des obsèques	Extrait de l'acte	
- des collatéraux du 2e degré (frère, sœur, beau-frère, belle-sœur)	3 jours ouvrables consécutifs dont le jour des obsèques	Extrait de l'acte	
- des autres ascendants ou descendants	2 jours ouvrables consécutifs dont le jour des obsèques	Extrait de l'acte	
- des collatéraux du 3e degré (oncles, tantes, neveux, nièces)	2 jours ouvrables consécutifs dont le jour des obsèques	Extrait de l'acte	

AUTORISATIONS EXCEPTIONNELLES D'ABSENCE

MOTIF	DURÉE MAXIMUM (en nombre de jours)	JUSTIFICATIF À FOURNIR	OBSERVATIONS
F - Autorisation exceptionnelle d'absence * - pour soigner un conjoint, le partenaire d'un PACS, le concubin, une personne à charge ou un ascendant ou atteint d'une maladie grave.	3 jours ouvrables		
- pour soigner un enfant malade ou en assurer momentanément la garde (âge limite 16 ans sauf si l'enfant est handicapé)	Plafond égal aux obligations hebdomadaires plus 1 jour, voire 2 fois les obligations hebdomadaires plus 2 jours quand le conjoint ne bénéficie pas des mêmes dispositions (fournir une attestation de l'employeur du conjoint)	Certificat médical pour l'enfant ou la personne en assurant la garde	Plafond par famille quel que soit le nombre d'enfants et octroyé à l'année civile.
G - Déménagement	1 jour	Pièce justificative de domicile	Concerne exclusivement le déménagement de l'agent.

Remarques :

- Pour les autorisations d'absence prévues au paragraphe F, l'agent dont le conjoint n'a pas d'activité professionnelle, ne peut bénéficier que d'une fois les obligations plus 1 jour.
- Les congés exceptionnels et les autorisations exceptionnelles d'absence n'ont lieu d'être accordés que dans la mesure où l'agent exerce ses fonctions au moment où les circonstances justifiant leur octroi se produisent. En conséquence, un congé exceptionnel ou une autorisation exceptionnelle d'absence ne peut être accordé à un agent en congé annuel et donc interrompre ce congé.
- Par jour ouvrable, il faut entendre tous les jours de la semaine, du lundi au samedi à l'exception des dimanches et des jours fériés chômés.
- Les agents publics ayant conclu un PACS se voient accorder toutes les autorisations d'absence pour motif familial dans les mêmes conditions.

** Ces absences ont vocation à être accordées lorsque l'agent se retrouve confronté à une situation imprévue face à laquelle il ne dispose pas d'autres moyens que l'utilisation de ces autorisations d'absence.*

ANNEXE 9 – Liste des agents bénéficiant à titre individuel de la reprise de leurs régimes de garde 12 heures tel qu'au 31 décembre 2013 (article 4200-13)

NOM	PRENOM	Temps de travail annuel	Nombre de gardes
~~ANDRIEU~~	~~Quentin~~	~~1596~~	~~133~~
GIBASSIER	Mathieu	1596	133
HAMARD	Laurent	1548	129
~~LENOIR~~	~~Yohann~~	~~1560~~	~~130~~
YAHIAOUI	Sylvain	1560	130
TOCQUEVILLE	Alain	1512	126
~~ANGOT~~	~~Pierre~~	~~1512~~	~~126~~
~~BURAY~~	~~Yannick~~	~~1512~~	~~126~~
NOEL	François	1512	126
PATIN	Olivier	1512	126
GOUBARD	Bruno	1524	127
ROQUET	Régis	1512	126
HUON	Pascal	1524	127
GUERECHE	Dominique	1512	126
~~HENRY~~	~~Jean-Luc~~	~~1512~~	~~126~~
~~QUESNE~~	~~Michel~~	~~1512~~	~~126~~
PERREAU	Jean-Louis	1536	128
PANLOUP	Vincent	1560	130
LUCAS	Sébastien	1524	127
HAUGUEL	Frédéric	1548	129
LEBOURG	Marc	[illegible]	128
GLARAN	Emmanuel	1572	131
JOUENNE	Stéphane	1584	132
MOREL	Éric	1524	127
~~GUBRI~~	~~Éric~~	~~1512~~	~~126~~
LAIGUILLON	Laurent	1524	127

ANNEXE 13 – Règlement départemental fixant les modalités allouées aux sapeurs-pompiers volontaires

ANNEXE 14 – Guide de la protection fonctionnelle

ANNEXE 15 – Charte de sécurité et du bon usage des ressources informatiques et numériques

Sapeurs-Pompiers
de Seine-Maritime

SDIS76

Annexe 14 du Règlement intérieur

Projet

Guide de la protection fonctionnelle

TYPE de Document
Règlement intérieur - Annexe 14
MAJ
07/04/2018

INTRODUCTION

Le présent guide a pour objet de décrire les modalités de mise en œuvre de la protection fonctionnelle (ou protection juridique) à laquelle ont droit les agents titulaires comme les non-titulaires en vertu de l'art 11 de la loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.

Ce guide pratique aborde les principes applicables, le déroulé de la procédure, le descriptif des pièces à fournir lors de la demande de protection fonctionnelle, la phase pénale.

Il n'a pas vocation à évoquer toutes les situations que pourraient rencontrer les agents départementaux dans l'exercice de leurs fonctions.

Coordonnées du Service des affaires juridiques :

02.35.56.11.11

juridique@sdis76.fr

1. DEFINITION

La loi du 13 juillet 1983 portant droits et obligations des fonctionnaires prévoit au bénéfice des agents une garantie de protection à l'occasion de leurs fonctions.

Cette protection constitue une obligation pour l'administration et un droit pour l'agent.

Cette protection revêt un double aspect : lorsque l'agent est victime et lorsque l'agent est mis en cause pénalement dabs l'exercice de ses fonctions.

Préalablement à l'exposé de la procédure, il convient de rappeler que la collectivité est tenue d'accorder sa protection à l'agent lorsque celui-ci a commis une faute de service.
La faute personnelle de l'agent ne lui permet pas de bénéficier de cette protection.

La faute personnelle *s'entend comme la faute commise par l'agent en dehors du service, ou pendant le service si incompatible avec le service public, les pratiques administratives normales qu'elle revêt une particulière gravité et est inexcusable notamment si elle est intentionnelle.*

La faute de service *est celle commise par un agent dans le cadre de ses fonctions, c'est-à-dire pendant le service, avec des moyens du service et en dehors de tout intérêt personnel.*

1.1 LE DISPOSITIF GENERAL

L'article 11 modifié de la loi n°83-634 du 11 juillet 1983 portant droits et obligations des fonctionnaires pose le principe d'une protection de l'agent public organisée par la collectivité publique dont il dépend lorsqu'il est victime d'agression physique ou verbale ou lorsqu'il est mis en cause pénalement ou poursuivi par un tiers pour une faute de service dans l'exercice de ses fonctions.

Cet article prévoit que la collectivité est tenue de protéger son agent lorsque :

- ✓ Celui-ci est victime d'atteintes volontaires à l'intégrité de sa personne, de violences, d'agissements constitutifs de harcèlement, de menaces, d'injures, de diffamations, d'outrages à raison de ses fonctions. Dans un souci de simplification, le terme « agression » sera utilisé dans le présent document pour désigner ces atteintes.

- ✓ Celui-ci est poursuivi civilement par un tiers pour une faute de service.
- ✓ Celui-ci fait l'objet de poursuites pénales à raison de fait qui n'ont pas le caractère d'une faute personnelle détachable de l'exercice de ses fonctions.

Cette protection est également accordée, sur leur demande, au conjoint, concubin ou partenaire lié par un PACS, aux enfants, aux ascendants directs pour les poursuites qu'ils engagent contre les auteurs d'atteintes volontaires à l'intégrité physique dont ils sont eux-mêmes victimes ou en cas d'atteinte à la vie du fonctionnaire parent du fait des fonctions exercées par le fonctionnaire.

1.2 AUTEUR DE LA PROTECTION

Conformément au I de l'article 11 de la loi n°83-634, la protection fonctionnelle est accordée par la collectivité employeur à la date des faits en cause ou des faits ayant été imputés de façon diffamatoire.

L'employeur à la date des faits accorde sa protection.

1.3 LA NATURE DE LA PROTECTION

Il appartient à chaque employeur de définir les modalités de mise en œuvre de la protection fonctionnelle. Ces modalités peuvent, de fait, être très variées, mais doivent cependant être adaptées à la situation.

Il revient à l'administration de mettre en œuvre la protection fonctionnelle afin de faire cesser les attaques, réparer les préjudices subis, mais également d'assister matériellement l'agent.

Il appartient à l'employeur de définir les modalités de mise en œuvre de la protection fonctionnelle.

1.4 LES BENEFICIARES

La protection fonctionnelle peut être accordée :

- ✓ *Aux fonctionnaires (stagiaires ou titulaires) et anciens fonctionnaires*
- ✓ *Aux agents contractuels et anciens agents contractuels*
- ✓ *Aux sapeurs-pompiers professionnels ou volontaires*
- ✓ *Aux anciens sapeurs-pompiers professionnels ou volontaires*

La protection est accordée par la collectivité employeur à la date des faits en cause.

La protection fonctionnelle peut aussi être accordée pour les instances qu'ils engagent contre les auteurs d'atteintes volontaires à l'intégrité de la personne dont ils sont eux-mêmes victimes du fait des fonctions exercées par le fonctionnaire sur leur demande :

- ✓ *Au conjoint, concubin, partenaire lié par un PACS,*
- ✓ *Aux enfants et ascendants directs,*
- ✓ *Au conjoint, concubin, partenaire lié par un PACS contre les auteurs d'atteinte volontaire à la vie du fonctionnaire du fait des fonctions exercées par celui-ci. A défaut d'action engagée par les personnes précitées, la protection peut être accordée aux enfants ou à défaut, aux ascendants directs du fonctionnaire qui engagent une telle action.*

Tous protégés

1.5 LE LIEN AVEC LES FONCTIONS

En application du premier alinéa de l'article 11, la protection n'est due qu' *« à raison de ses fonctions »*. Ainsi, les atteintes ou la mise en cause pénale doivent nécessairement être dirigées contre l'agent à l'occasion de ses fonctions ou du fait de sa qualité de fonctionnaire.

1.6 LES CAS DE MISE EN ŒUVRE DE LA PROTECTION FONCTIONNELLE

1.6.1 *La protection en cas d'atteintes volontaires à l'intégrité de la personne, de violences, d'agissements constitutifs de harcèlement, de menaces, d'injures, de diffamations ou d'outrages dont l'agent pourrait être victime sans qu'une faute personnelle puisse lui être imputée.*

➢ **L'origine des atteintes :**

Les atteintes peuvent aussi bien émaner de personnes privées, de tiers ou d'usagers du service que d'agents publics ou autorités de toute nature.

➢ **La nature des atteintes :**

Le droit à protection est ouvert lorsque vous êtes victime d

- ***Menaces :*** *intimidation ou pression ayant pour objet une atteinte aux personnes ou aux biens (exemple : menace de mort)*
- ***Violences :*** *ensemble des actes portant atteinte à l'intégrité des individus*
- ***Injures :*** *expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait précis*
- ***Diffamation :*** *allégation ou imputation d'un fait, constitutive d'un délit qui porte atteinte à l'honneur ou à la considération d'une personne ou d'un corps constitué*
- ***Outrages :*** *expression menaçante, diffamatoire ou injure propre à diminuer l'autorité morale de la personne investie d'une fonction de caractère public.*
- ***Atteintes visant l'intégrité physique ou la vie de l'agent public***
- ***Atteintes mettant en cause l'honneur de l'agent ou son comportement***
- ***Atteintes aux biens***
- ***Harcèlement :*** *comportements répétés qui ont pour objet ou pour effet une dégradation des conditions de travail susceptible de porter atteinte aux droits du salarié et à sa dignité, d'altérer sa santé physique ou mentale, ou de compromettre son avenir professionnel.*

1.6.2 *La protection en cas de poursuites pour faute de service ou de poursuites pénales*

En plus des infractions mentionnées ci-dessus, les II et III de l'article 11 de la loi du 13 juillet 1983 prévoient que l'agent poursuivi par un tiers pour faute de service bénéficient de la protection fonctionnelle.

En cas de poursuites pour faute de service, l'agent a droit à la protection fonctionnelle lorsque les faits commis par lui sont constitutifs d'une faute de service et exclusifs de toute faute personnelle détachable de l'exercice des fonctions.

Exemple de fautes de service : **Une mauvaise organisation du service, des dommages pouvant provenir d'erreurs, de négligences, l'inertie de l'administration due a une absence de fonctionnement du service, le non-respect de prescriptions réglementaires concernant des locaux.**

En revanche, dès lors que les faits reprochés à l'agent peuvent être qualifiés de faute personnelle, la protection fonctionnelle ne peut pas lui être accordée.

Exemple de fautes personnelles : **Conduire sous l'emprise d'un état alcoolique pendant les heures de service, commettre un crime, tenir des propos injurieux à l'égard d'un collègue, détourner des fonds publics, établir un faux en écriture pour obtenir un avantage.**

De la même façon, en cas de poursuites pénales engagées contre un agent, l'octroi de la protection fonctionnelle est conditionnée au fait que l'agent fasse l'objet de poursuites à l'occasion de faits n'ayant pas le caractère de faute personnelle. Elle est donc limitée au cas où l'infraction à l'origine des poursuites est constitutive d'une faute de service.

La protection est accordée uniquement en cas de faute de service.

Le point de départ des poursuites pénales correspond à la date de mise en mouvement de l'action publique par le Parquet à l'encontre de l'agent.

La protection fonctionnelle doit donc être mise en œuvre au profit d'un agent mis en examen, entendu comme témoin assisté, gardé à vue, faisant l'objet d'une citation directe, convoqué dans le cadre d'une procédure de comparution sur reconnaissance préalable de culpabilité.

Qu'il s'agisse de la protection accordée à l'agent poursuivi par un tiers pour faute de service ou de la protection due à l'agent pénalement poursuivi pour des faits constitutifs de fautes de service, la collectivité, dans l'hypothèse où l'agent serait condamné, doit le couvrir des éventuelles condamnations civiles prononcées à son encontre.

L'autorité d'emploi ne peut supporter que les condamnations civiles (*amendes pénales exclues*)

1.7 LA MATERIALITE DES FAITS

Il appartient à l'agent qui sollicite le bénéfice de la protection fonctionnelle d'établir l'origine et la matérialité des faits dont il se dit victime.

Lorsqu'il est mis en cause pénalement, il doit également établir en quoi les poursuites dont il fait l'objet sont en lien avec le service.

1.8 LES LIMITES DE LA PROTECTION FONCTIONNELLE

La protection fonctionnelle est un droit pour les fonctionnaires titulaires ou stagiaires et les agents publics. Cependant, dans certains cas, l'administration est en droit de refuser la protection fonctionnelle.

- Lorsque les conditions légales ne sont pas réunies, à savoir, pour les agents mis en cause, en cas de faute personnelle détachable de l'exercice des fonctions,
- Pour les agents victimes, la jurisprudence admet qu'en présence de motifs d'intérêt général, la protection fonctionnelle pouvait être refusée.

À titre d'exemple, caractérise un motif d'intérêt général, le fait pour un agent d'avoir une part de responsabilité dans le climat gravement et durablement conflictuel du service au sein duquel il travaille.

2. LA PROCEDURE

2.1 LA MISE EN ŒUVRE DE LA PROTECTION FONCTIONNELLE

2.1.1 La demande formulée par l'agent

L'agent victime d'atteintes ou l'agent mis en cause pénalement dans l'exercice de ses missions doit, s'il souhaite bénéficier de la protection fonctionnelle, formuler sa demande par écrit au Président du Conseil d'administration du Sdis 76.

La protection fonctionnelle ne peut donc être mise en œuvre que si l'agent en fait la demande (*cf. annexe n°2*) et qu'après que le Président du Conseil d'administration du Sdis ait reçu l'accord du Bureau du Conseil d'administration d'engager les dépenses afférentes à sa mise en œuvre.

Pour prétendre à la protection fonctionnelle, l'agent doit établir la matérialité des faits dont il se dit victime et le préjudice direct qu'il a subi. Il doit fournir tous les éléments d'information et donner tous les justificatifs concernant les faits et circonstances motivant sa demande.

L'agent doit demander par écrit le bénéfice de la protection fonctionnelle

A la réception de la demande de protection fonctionnelle qui sera transmise au SAJ par le supérieur hiérarchique de l'agent, l'organe délibérant sera saisi du dossier.

L'agent sera informé par la suite par courrier du Président du Conseil d'administration quant à l'octroi ou non de la protection fonctionnelle.

Une fois, la protection accordée, le SAJ prend en charge la gestion du dossier et accompagne l'agent dans toutes les étapes et répond aux questions qu'il pourrait se poser.

L'agent pourra demander à être représenté par un avocat de son choix ou conseillé par le service, une convention d'honoraires devra alors être rédigée, cependant, le Sdis pourra décider de ne régler qu'une partie des honoraires si ces derniers sont manifestement excessifs.

Une fois l'avocat désigné, une rencontre pourra être organisée avec l'agent afin d'échanger sur le dossier.

2.1.2 Les démarches à effectuer

① *Agent victime*

Information du supérieur hiérarchique sur l'agression

Avant même d'effectuer les premières démarches, l'agent doit informer IMPERATIVEMENT son supérieur hiérarchique dès que l'agression a eu lieu. Il est le premier interlocuteur privilégié avant qu'il informe le pôle juridique – service des affaires juridiques.

Pour les sapeurs-pompiers victimes d'infraction en intervention, ils en réfèrent à leur COS.

Le certificat médical (uniquement en cas de violences physiques)

Lors d'une agression physique et afin de faire constater le plus rapidement les blessures, un examen médical doit être pratiqué par un médecin du choix de l'agent qui constatera les lésions consécutives à l'agression et rédigera un certificat médical.

Ce dernier va préciser le nombre de jours éventuels d'incapacité temporaire de travail (ITT).

L'incapacité temporaire de travail (ITT) est la durée pendant laquelle une victime éprouve une gêne notable dans les actes de la vie courante, elle permet de qualifier pénalement un acte violent.

L'ITT ne doit pas être confondue avec la durée de l'arrêt de travail qui correspond à la constatation d'un état de santé qui n'est pas compatible avec la pratique du travail. Ainsi, un agent ayant subi une agression peut se voir reconnaître un ITT de 3 jours et avoir un arrêt de travail d'une semaine.

Les documents médicaux (Arrêt de travail et ITT) devront être transmis dans les plus brefs délais au Service départemental d'incendie et de secours.

Le dépôt de plainte

Le dépôt de plainte est l'acte par lequel une personne qui s'estime victime d'une infraction pénale en informe la justice. La plainte est déposée contre une personne identifiée ou contre X, si l'identité de l'auteur des faits est inconnue.

La plainte permet de demander une sanction pénale (prison, amende…) contre l'auteur des faits.

Systématiquement, lorsqu'un agent du Sdis 76 dépose plainte pour agression dans le cadre de ses fonctions, le Sdis 76 dépose également plainte au nom du Service afin d'appuyer la démarche de l'agent.

Pour obtenir réparation du préjudice (remboursement d'objet volés, dommages et intérêts…) la plainte ne suffit pas, il faut se constituer partie civile.

Le dépôt de plainte est enfermé par des délais qui varient suivant la gravité de l'infraction, néanmoins, il est conseillé de déposer plainte dans les plus brefs délais après la commission des faits auprès des services territorialement compétents

Pour un meilleur suivi du dossier et afin également de protéger les agents, il est impératif que chaque agent victime d'une infraction en raison de ses fonctions se domicilie à la direction départementale des services d'incendie et de secours de la Seine-Maritime, 6 rue du verger, 76190 YVETOT.

Afin de vous garantir un meilleur traitement de votre dossier, il est impératif qu'une copie du dépôt de plainte soit transmise au SAJ via le chef de centre ou le chef de service.

Domiciliation de l'agent à la direction départementale

② *Agent mis en cause*

Information du supérieur hiérarchique de la mise en cause

Dès réception d'une convocation, l'agent doit informer IMPERATIVEMENT son supérieur hiérarchique. Il est le premier interlocuteur privilégié avant qu'il informe le pôle juridique – service des affaires juridiques.

Préparation de la défense de l'agent

Informé par le supérieur hiérarchique, le pôle juridique – service des affaires juridiques prendra contact avec l'agent afin de l'informer de la procédure engagée à son encontre. La désignation d'un avocat pour défendre les intérêts de l'agent sera rapidement engagée afin qu'un rendez-vous entre l'agent mis en cause, l'avocat et le service des affaires juridiques soit pris pour définir les axes de défense.

3. LE DEROULEMENT DE LA PHASE PENALE

3.1 Préparation de l'audience

L'agent peut préparer l'audience avec l'avocat qu'il aura choisi ou l'avocat proposé par le service. Sur demande de l'agent, une réunion préalable avec le SAJ peut être organisée.

Cette rencontre est destinée à expliquer à l'agent le déroulement de l'audience et à répondre à ses interrogations et à celles des éventuels témoins.

3.2 L'audience

Le jour de l'audience, l'avocat choisi assurera la représentation de l'agent. La présence de la victime n'est pas obligatoire. Cependant lorsque la victime est présente, le juge peut l'interroger afin de mieux circonscrire l'évènement ayant donné lieu aux poursuites.

Dans le cas d'une mise en cause, la présence de l'agent est obligatoire dans la perspective d'appuyer sa défense.

La présence de l'agent à l'audience est souhaitable pour répondre aux éventuelles questions du magistrat

Lorsque l'agent se déplace à l'audience, il est systématiquement accompagné par un agent du SAJ sauf si ce dernier ne le souhaite pas.

Le délibéré (décision du tribunal) est soit rendu le jour même, soit à une date ultérieure. L'avocat informera l'agent de la décision rendue, le SAJ informe votre hiérarchie.

A réception du jugement rendu exécutoire, c'est-à-dire opposable à l'auteur des faits, l'avocat vous conseille sur l'opportunité ou non de faire appel de la décision. En cas d'appel (du Procureur, de l'auteur des faits ou de vous), le même avocat assurera la défense de vos intérêts.

3.3 L'exécution du jugement

Une fois le jugement rendu exécutoire (ce qui peut prendre plusieurs mois après la date d'audience), l'avocat qui a défendu les intérêts de l'agent prend contact avec l'avocat de l'auteur des faits afin d'envisager l'exécution du jugement de façon amiable. A défaut, un huissier de justice peut être saisi par le service pour recouvrer les sommes dues.

Ces démarches sont souvent très longues et indépendantes de la volonté du Sdis. Cette longueur de traitement peut susciter de la frustration chez les victimes qui éprouvent des difficultés à obtenir réparation de leur préjudice.

En cas d'inexécution avérée du jugement, le Sdis76 réparera le préjudice de son agent victime et sera subrogé dans ses droits pour obtenir le paiement des sommes versées à son agent. Lorsque le SAJ constate l'échec à exécution, il contacte la victime et lui adresse une demande de réparation de préjudice (annexe n° 3).

En l'absence du document dûment complété, le Sdis ne pourra pas procéder à l'indemnisation de l'agent.

4. L'ASSISTANCE DU POLE JURIDIQUE – SERVICE DES AFFAIRES JURIDIQUES

Le service des affaires juridiques est l'interlocuteur privilégié de l'agent victime, et celui de ses supérieurs hiérarchiques.

Le SAJ suit toute la procédure, et donne toutes les instructions et renseignements utiles à l'avocat en charge du dossier. Il assure et informe l'agent du suivi de l'action judiciaire, en liaison directe avec sa hiérarchie.

Pièces du dossier pour un agent victime :

- ☐ **La copie du dépôt de plainte**
- ☐ **Le certificat médical le cas échéant avec nombre d'ITT**
- ☐ **Une copie de l'avis à victime / avis d'audience (*s'il a été adressé directement à l'agent ou au Cis suivant l'adresse indiquée dans le dépôt de plainte*)**
- ☐ **La demande de protection fonctionnelle**
- ☐ **La constitution de partie civile**

Pièces du dossier pour un agent mis en cause :

- ☐ **La copie de la convocation au tribunal / information de la mise en cause**
- ☐ **La demande de protection fonctionnelle**
- ☐ **Tout élément pouvant être pertinent pour la défense de l'agent (compte-rendu, témoins……)**

*

**

Le SAJ accompagne l'agent tout au long de la procédure jusqu'à l'exécution totale du jugement, il reste à l'écoute de chaque agent pendant la procédure.

Les agents qui le désirent peuvent demander un rendez-vous auprès des agents du SAJ afin que ces derniers leur expliquent la procédure.

Le SAJ assure également le suivi de l'exécution du jugement et met en œuvre l'indemnisation des victimes en cas d'échec à exécution.

Le Service des affaires juridiques accompagne l'agent tout au long de la procédure

ANNEXES

ANNEXE 1 : Tableaux récapitulatifs

ANNEXE 2 : Modèle de demande de protection fonctionnelle

ANNEXE 3 : Modèle de constitution de partie civile

ANNEXE 4 : Modèle de demande de réparation du préjudice

ANNEXE 1

Tableaux récapitulatifs

1. DEMARCHES A SUIVRE LORSQUE L'AGENT EST VICTIME D'UNE AGRESSION DANS L'EXERCICE DE SES FONCTIONS

Nature	Comment	Où	Quand et par qui ?	Bon à savoir
Agression physique ou verbale	**1°) Information du supérieur hiérarchique**		Par l'agent, le COS ou par le CTA-CODIS immédiatement après la commission des faits.	
	2°) Certificat médical (uniquement en cas de violences physiques)	Centre hospitalier, CASA ou cabinet du médecin traitant	Immédiatement après l'agression par un médecin de son choix	✓ Le certificat médical précisera le nombre d'ITT qui permet de déterminer la qualification pénale
	3°) Dépôt de plainte : Au nom de l'agent contre X ou contre l'auteur connu	Commissariat ou gendarmerie territorialement compétent	Rapidement après la commission des faits par l'agent	✓ Dans le dépôt de plainte, **l'agent doit se domicilier à la direction départementale** des services d'incendie et de secours
	Au nom du Sdis 76 contre X ou contre l'auteur connu	Force de l'ordre recevant la plainte de l'agent ou auprès du Procureur de la République Tribunal de Grande Instance compétent	Après les dépôts de plaintes des agents par le chef de groupe, chef de centre ou le SAJ	✓ L'agent qui dépose plainte doit récupérer une copie du procès-verbal d'infraction et le transmettre au SAJ par voie hiérarchique
La protection fonctionnelle	Par lettre à l'attention du Président du conseil d'administration (cf annexe 1)		Dès réception de l'avis à victime ou l'avis d'audience, La demande de l'agent est transmise au SAJ par voie hiérarchique	✓ Le bureau du conseil d'administration doit autoriser le Président à engager les frais relatifs à la procédure ✓ Le SAJ informe l'agent de la décision du bureau du conseil d'administration ✓ Elle est accordée aux titulaires comme aux non-titulaires ✓ Les frais d'avocats sont pris en charge par le Sdis 76 ✓ En cas d'inexécution du jugement, le Sdis indemnisera l'agent de son préjudice

2. DEMARCHES A SUIVRE LORSQUE L'AGENT EST MIS EN CAUSE PENALEMENT DANS L'EXERCICE DE SES FONCTIONS

Nature	Comment	Où	Quand et par qui ?	Bon à savoir
Mise en cause pénalement ou civilement de l'agent dans l'exercice de ses fonctions	**1°) Information du supérieur hiérarchique**		Par l'agent Immédiatement après la connaissance de la procédure engagée à son encontre	
La protection fonctionnelle	Par lettre à l'attention du Président du conseil d'administration (cf annexe 1)		Dès la mise en cause de l'agent	✓ La protection est accordée à l'agent **s'il n'a pas commis de faute personnelle.** En cas de faute personnelle de l'agent, la collectivité doit refuser sa protection ✓ Dans le cadre de la défense, les frais d'avocat sont pris en charge par le Sdis 76 ✓ Le Sdis prendra en charge les condamnations civiles de l'agent mais **pas les amendes**

ANNEXE 2

Demande de protection fonctionnelle

Agent victime

[*Ville*], le

Grade NOM Prénom
CIS
coordonnées
Tel:

Monsieur le Président du Conseil
d'administration du Sdis 76
6 rue du verger
CS 40078
76192 YVETOT Cedex

Monsieur le Président,

Par la présente, je sollicite auprès du Service départemental d'incendie et de secours de la Seine-Maritime le bénéfice de la protection fonctionnelle. J'ai en effet été victime de …….[*faits*]……, le XX/XX/XXXX…[*date*]….., lors d'une intervention sur la commune de ….[*Ville*]…. L'auteur des faits a été identifié et une audience se tiendra devant le Tribunal de Grande Instance de …….[*Ville de l'audience*]…… le XX/XX/XXXX…[*date*]….

Veuillez agréer, Monsieur le Président, l'expression de ma considération distinguée.

Nom et signature de l'agent

Agent mis en cause

[*Ville*], le

Grade NOM Prénom
CIS
coordonnées
Tel:

Monsieur le Président du Conseil
d'administration du Sdis 76
6 rue du verger
CS 40078
76192 YVETOT Cedex

Monsieur le Président,

Par la présente, je sollicite auprès du Service départemental d'incendie et de secours de la Seine-Maritime le bénéfice de la protection fonctionnelle. Je suis mis en cause pour .....[*qualification pénale*]....., pour des faits qui se sont déroulés le XX/XX/XXXX…[*date*]....., à de.....[*circonstances*]..... . Le procureur de la République a été saisi des faits et une audience se tiendra devant le Tribunal de Grande Instance de .....[*Ville de l'audience*]..... le XX/XX/XXXX…[*date*].... .

Veuillez agréer, Monsieur le Président, l'expression de ma considération distinguée.

Nom et signature de l'agent

Guide de la protection fonctionnelle

ANNEXE 3

Constitution de partie civile

[Ville], le

Grade NOM Prénom
CIS
coordonnées
Tel:

Monsieur le Procureur de la République
Tribunal de Grande Instance de Rouen
1 Place du Maréchal FOCH
76000 ROUEN

Monsieur le Procureur,

J'ai été victime de ….. [*qualification pénale*]……, le XX/XX/XXXX…..[d*ate*]……, lors d'une intervention sur la commune de …[*Ville*]. … L'auteur des faits a été identifié, il s'agit de [*civilité NOM Prénom*] et une audience se tiendra devant le Tribunal de Grande Instance le XX/XX/XXXX…[*date*]….

Par la présente, j'entends me constituer partie civile dans ce dossier et je sollicite une indemnisation de *XXX euros* (*à préciser*) en réparation du préjudice subi.

Veuillez agréer, Monsieur le Procureur, l'expression de ma considération distinguée.

Nom, Prénom et signature de l'agent

ANNEXE 4

Demande de réparation de préjudice

NOM Prénom

Cis

coordonnées

Ville, date

Monsieur Le Président du conseil
d'administration du Service départemental
d'incendie et de secours de la Seine-
Maritime

Référence : Référence dossier

Objet : Demande de réparation du préjudice

Monsieur le Président,

Sur le fondement de l'obligation de garantie des agents contre les risques que comportent leurs fonctions, j'ai l'honneur de solliciter la réparation pécuniaire du préjudice que j'ai subi le à l'occasion de l'exercice de mes fonctions.

Selon le jugement rendu le *[date]*..... par le tribunal de grande instance de...*[Ville]*....., dont copie jointe, ...[*NOM, Prénom auteur des faits*]..... a été reconnu coupable de .....[*qualification des faits*]....., et condamné à me payer la somme de .....[*montant*]..... € à titre de dommages-intérêts.

Malgré les relances réalisées, le préjudice subi n'a pas été / n'a pas été intégralement réparé.

Je sollicite donc le versement de la somme de .....[*Montant restant dû*]..... € à titre de réparation.

J'ai l'honneur de solliciter de votre bienveillance quant à l'examen de ma demande.

Nom, Prénom et signature de l'agent

Sapeurs-Pompiers
de Seine-Maritime

SDIS76

Annexe 15 du Règlement intérieur

-

Charte de sécurité informatique et du bon usage des ressources informatiques et numériques

Projet

TYPE de Document
Règlement intérieur - Annexe 15
MAJ
07/04/2018

SOMMAIRE

TEXTES APPLICABLES

- *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*
- *Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil*
- *Loi du 29 juillet 1881 sur la liberté de la presse, notamment le chapitre IV,*
- *Loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et les actes réglementaires pris en application de son article 15 pour autoriser la mise en œuvre de traitements informatiques,*
- *Loi n°83-634 du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires, notamment art.6 (liberté d'opinion), 8 (droit syndical) et 26 (obligations de discrétion et de secret professionnels, auxquelles sont rattachées les obligations de réserve et de neutralité),*
- *Loi n°84-16 du 11 janvier 1984 modifiée portant obligations statutaires relatives à la fonction publique de l'État,*
- *Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,*
- *Loi du 5 janvier 1988 dite « Godfrain » relative à la fraude informatique,*
- *Loi (646) du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications,*
- *Loi du 15 novembre 2001 relative à la sécurité quotidienne (LSQ),*
- *Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité (LOPPSI 2),*
- *Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet (HADOPI).*
- *Code civil, art. 9 (respect de la vie privée),*
- *Code pénal, notamment art. 226-1 à 226-7 (atteintes à la vie privée), 226-13 à 226-14 (atteintes au secret professionnel), 226-15 et 432-9 (atteintes au secret des correspondances), 226-16 à 226-24 (atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques), 323-1 à 323-7 (atteintes aux systèmes de traitement automatisés de données),*
- *Code de la propriété intellectuelle, notamment art.L112-1 à L112-3 (œuvres protégées), L335-1 à L335-9,*

FINALITE ET OBJECTIFS

La présente charte est un document structurant de l'établissement ayant pour finalité de définir les règles d'utilisation et de préciser les responsabilités des utilisateurs et des administrateurs conformément à la législation en vigueur, et de permettre ainsi un usage normal, optimal et sécurisé des ressources informatiques et téléphoniques mises à leur disposition.

Elle constitue une annexe au règlement intérieur du Service départemental d'incendie et de secours de la Seine-Maritime (Sdis 76), prévu par l'article R 1424-22 du code général des collectivités territoriales.

La charte a été réalisée afin de répondre à deux objectifs principaux :

- *assurer la sécurisation des systèmes d'information et de communication du Sdis 76 et par conséquent la sauvegarde et la confidentialité des données stratégiques,*
- *assurer une utilisation adéquate et loyale des différentes ressources informatiques et téléphoniques.*

Elle est donc destinée à établir des règles opposables et transparentes aux personnels et utilisateurs collectifs, en apportant des restrictions légitimes et proportionnées aux droits des personnes et aux libertés individuelles et collectives, dans le strict respect du droit.

La volonté du Sdis est d'instaurer, en accord avec la législation, un usage correct des ressources informatiques et de communication mises à disposition des utilisateurs. La sécurité étant l'affaire de tous, chaque utilisateur des moyens informatiques et de communication du Sdis doit y contribuer en mettant en application les règles énoncées dans cette charte. Le Sdis 76 compte donc sur l'implication de chaque utilisateur pour permettre la réussite de cette démarche et assurer la poursuite de ses objectifs de sécurité et de qualité de service.

CHAMP D'APPLICATION

Les dispositions de la présente charte s'appliquent à l'ensemble des agents du Sdis 76, quelle que soit leur position statutaire :

- les sapeurs-pompiers professionnels ;
- les sapeurs-pompiers volontaires ;
- les fonctionnaires titulaires ou stagiaires ne relevant pas de la filière des sapeurs-pompiers professionnels ;
- les agents non titulaires ne relevant pas de la filière des sapeurs-pompiers professionnels.

La charte concerne également l'ensemble des élus du Sdis 76, des intervenants intérimaires, stagiaires, apprentis et des intervenants extérieurs temporairement autorisés (*élus et agents d'autres collectivités territoriales, agents de la fonction publique d'état, collaborateurs d'associations, prestataires*).

La présente charte porte à connaissance de l'utilisateur les principales règles et bonnes pratiques à adopter pour un usage correct, loyal et sécurisé des ressources actuelles et futures mises à sa disposition.
Elle annule et remplace la version de la précédente charte éditée en 2008.

Elle définit les conditions générales d'utilisation des services Internet, des réseaux informatiques, des services multimédias, du web (réseaux sociaux, blogs, wikis, forums, etc.) et plus généralement des moyens de communications au sein du Sdis 76 conformément au cadre légal et réglementaire en vue de sensibiliser et de responsabiliser l'utilisateur. Elle vise également à informer les utilisateurs des contrôles mis en place.

PREAMBULE

Administrateur des systèmes d'informations :

On entend par administrateurs, l'ensemble des personnes, quel que soit leur statut (interne comme externe), ayant en charge :

- des actions d'administration ou d'exploitation, incluant l'installation, la configuration, la maintenance, le support et l'évolution,
- des actions de sécurisation et de contrôle des ressources physiques et logiques des systèmes d'information de l'établissement : ressources systèmes, réseaux, serveurs, téléphonie, bureautique (postes de travail et leurs périphériques) et applications (et ce compris les bases de données).

Les administrateurs du Sdis 76 travaillent au sein du groupement des Systèmes d'informations (GSI) et veillent à la protection, à la maintenance et au bon fonctionnement des systèmes d'informations.

L'administrateur est tenu à un devoir de réserve. Il ne peut divulguer les informations auxquelles il a accès de par ses droits de supervision.

Utilisateur :

L'utilisateur est toute personne, quel que soit son statut (*élu, agent permanent, agent temporaire, intérimaire, stagiaire, apprenti et intervenant extérieur temporairement autorisé*) qui est amené à accéder et utiliser les ressources informatiques mises à sa disposition pour assurer sa mission.

CHAPITRE 1 : STATUT DE LA CHARTE

ARTICLE 1 – Application de la charte

La charte est diffusée à l'ensemble du personnel du Sdis 76, consultable sur l'intranet de l'établissement. L'utilisateur s'engage à prendre connaissance et à appliquer l'ensemble des dispositions de la présente charte.

Pour les agents du Sdis 76, la présente charte fait partie intégrante du règlement intérieur. Elle est par ailleurs remise à tout intervenant extérieur et sous-traitant commissionné sous couvert des autorités en charge, lesquelles s'engagent à sa stricte application.

Les contrats entre le Sdis 76 et tout tiers donnant accès aux données, aux programmes informatiques ou autres moyens devront stipuler que les utilisateurs s'engagent à respecter la présente charte.

Les responsables des utilisateurs extérieurs s'engagent à faire respecter la présente charte par leurs propres agents et éventuelles entreprises sous-traitantes.

Le GSI s'engage, pour sa part, à mettre en œuvre tous les moyens pertinents compte tenu de l'état des techniques, afin de garantir la meilleure sécurité possible des installations mises à la disposition des utilisateurs.

ARTICLE 2 – Responsabilités et sanctions

Article 2.1 – Responsabilités de l'établissement

Le Sdis déclare mettre en œuvre, par le biais de la présente charte et des diverses mesures de sécurité physique et logique qui sont les siennes, tous les efforts nécessaires à un bon usage de ses systèmes et du réseau et n'assumer aucune responsabilité au titre des agissements fautifs ou délictueux des utilisateurs auxquels il fournit un droit d'accès.

Article 2.2 – Responsabilités de l'utilisateur

Chaque utilisateur utilise les moyens informatiques et de téléphonie auxquels il a accès sous sa propre responsabilité. Il reconnait que toute violation des dispositions de la présente charte ainsi que, plus généralement, tout dommage créé au Sdis ou à des tiers de son fait engagera sa responsabilité, tant sur le plan disciplinaire, que civil ou pénal et s'expose à des sanctions. En outre, le Sdis se réserve le droit d'exercer une action contre l'utilisateur frauduleux afin d'obtenir réparation des préjudices directs ou indirects subis.

Article 2.3 – Responsabilités de l'administrateur

Le non-respect des règles édictées dans la présente charte engage la responsabilité des administrateurs et les expose, de manière appropriée et proportionnée au manquement commis, aux procédures disciplinaires applicables dans le cadre du Sdis et, pour les personnels externes, à toutes autres sanctions prévues conformément aux dispositions contractuelles.

La gravité des agissements constatés peut justifier le cas échéant la suspension immédiate, partielle ou totale, des prérogatives dévolues dans le cadre des missions concernées par les faits. On note toutefois que, nonobstant le changement ou la perte des attributions fonctionnelles, les obligations décrites dans la présente charte perdurent sans limite de temps, en particulier les obligations de confidentialités portant sur les données dont les administrateurs ont pu avoir connaissance au cours de leurs missions.

Article 2.4 – Poursuites et sanctions

Chaque utilisateur est responsable pénalement, selon les dispositions prévues au code pénal, pour les infractions qu'il aurait commises par ou au moyen des outils informatiques ou des moyens de communication mis à disposition.

De plus, chaque utilisateur est responsable civilement pour les dommages qu'il aurait causés par ou au moyen des outils informatiques ou des moyens de communication mis à disposition, pour autant qu'il s'agisse d'une faute lourde, d'un dol ou d'une faute légère ayant un caractère répétitif.

Cela signifie que l'usage abusif ou illicite des moyens de communication et des ressources informatiques mis à disposition par le Sdis 76 peut donner lieu au dépôt d'une plainte en justice ou une requête en indemnisation du dommage.

Enfin, le non-respect des règles et mesures de sécurité figurant dans la présente charte expose l'utilisateur, selon la gravité des infractions et leurs répercussions :

- *à un simple rappel aux bonnes pratiques ;*
- *à des mesures disciplinaires;*
- *à des poursuites pénales conformément aux dispositions légales en vigueur.*

CHAPITRE 2 : REGLES D'UTILISATION DES RESSOURCES

ARTICLE 3 – Règles d'utilisation des matériels, programmes et logiciels

Article 3.1 – Règles générales d'utilisation des ressources informatiques

Les unités de stockage du poste de travail de l'utilisateur (*disque dur, disque amovible, clé USB, etc.*) ne doivent pas contenir de programmes, logiciels, documents, fichiers, informations ou données à caractère illicite et peuvent faire l'objet de vérifications et de contrôles par le service, dans les limites prévues par la loi en matière de protection de la vie privée et par la présente charte.

Tous usages abusifs ou illicites des moyens de communication ou des outils informatiques mis à disposition sont interdits et peuvent être punis de sanctions prévues à l'article 2 de la présente charte.

Il faut entendre par «usage abusif ou illicite», l'usage répété durant et/ou en dehors des heures normales de travail des moyens de communication ou des ressources informatiques mis à disposition par le Sdis 76 à des fins non professionnelles, à l'exception de l'usage expressément autorisé par le supérieur hiérarchique.

On entend par «finalités non professionnelles», les finalités qui n'ont aucun lien direct avec les activités pour lesquelles l'utilisateur a été engagé.

Les moyens de communication et les outils informatiques sont utilisés principalement à des fins professionnelles et à titre subsidiaire à des fins personnelles sur le lieu de travail à condition que l'usage soit raisonnable.

Par usage professionnel on entend toute utilisation ayant un lien direct avec les activités pour lesquelles l'agent a été recruté.

L'usage durant et/ou en dehors des heures normales de travail des moyens de communication ou des ressources informatiques mis à disposition pour des finalités contraires à toute législation française ou internationale, à l'ordre public et aux bonnes mœurs ou pour des finalités qui sont susceptibles d'être sanctionnées, par voie pénale ou autre, par une autorité française ou une quelconque autorité étrangère, est interdit.

De manière plus générale, il est interdit de faire usage des moyens de communication ou des ressources informatiques mis à disposition dans un but contraire aux principes repris dans la présente charte ou aux instructions ou directives données par le supérieur hiérarchique.

L'utilisation de moyens de chiffrement à titre privé est interdite sur les ressources informatiques mises à disposition. Ainsi, tous les fichiers et répertoires sécurisés à l'aide d'un moyen de chiffrement doivent l'être à partir d'outils fournis par le service et sont réputés contenir exclusivement des données professionnelles.

Article 3.2 – Introduction de nouveaux matériels, programmes et logiciels

L'utilisateur n'est en aucun cas habilité à installer des logiciels, programmes ou nouveaux équipements.
L'installation de logiciels sur des ordinateurs reliés au réseau informatique du Sdis 76 est de la compétence exclusive du GSI. Les utilisateurs s'engagent à respecter la législation en vigueur sur la reproduction et le copyright des logiciels.

Conformément aux obligations de confidentialité d'application pour tous les agents, il n'est pas permis de vendre ou de transférer des logiciels, de la documentation associée ou tout autre type d'informations ou données internes vers une autre personne ou organisation sauf accord écrit du Directeur départemental.

Les échanges d'information, de logiciels et/ou de données entre Sdis 76 et une tierce partie ne peuvent avoir lieu sauf si cela est autorisé par la loi (notamment dans le cadre des missions de service public) ou si un contrat a été préalablement signé entre le Sdis 76 et cette tierce partie.
De tels contrats doivent spécifier les termes de l'échange et comporter une description claire de la manière dont seront traités l'information, le logiciel et/ou les données par la tierce partie.

Article 3.3 – Information à caractère privé sur les unités de stockage *(disque dur, disque amovible, clé USB, etc.)*

Les supports personnels ne sont pas autorisés sauf sur dérogation approuvée par le Directeur départemental. Les utilisateurs conserveront toute information privée dans un dossier privé clairement identifié comme tel. **Dans ce cas, l'utilisateur fera apparaître dans la dénomination du dossier, la mention : « PRIVE » ou « PERSONNEL ».**

Lorsque l'utilisateur quitte définitivement le Sdis 76, il doit procéder à la suppression de l'ensemble de ses fichiers privés. A défaut, il reconnaît au Service, le droit de les détruire.

L'utilisateur s'engage à ne pas détourner l'information professionnelle dont il a la charge en la qualifiant frauduleusement d'informations privées. De tels agissements exposent l'utilisateur aux sanctions prévues dans l'article 2 de la présente charte.

Article 3.4 – Accès extérieur

Lorsque l'utilisateur doit accéder au système d'information, en dehors des locaux du Sdis 76. Il devra activer les moyens de communication sécurisés fournis par le service pour accéder à distance aux ressources informatiques du Sdis 76. Les équipements informatiques fournis sont équipés des dispositifs techniques de sécurité. L'utilisateur ne doit en aucun cas désactiver les fonctions de sécurité mises en œuvre.

Article 3.5 – Règles d'utilisation des tablettes tactiles et des smartphones

Les tablettes tactiles et les smartphones sont des outils attitrés individuellement à l'utilisateur pour un usage exclusivement professionnel. De ce fait, leur utilisation est limitée au seul utilisateur à qui elle a été remise.

La signature de la présente charte engage ce dernier à mettre en œuvre toutes les mesures possibles pour :

- *s'assurer de ne pas laisser les équipements dans un endroit sans surveillance afin d'en prévenir le vol,*
- *ne jamais divulguer à quiconque son code PIN, ni son mot de passe de connexion au réseau et/ou aux applications métiers installées sur les appareils,*
- *avertir le GSI en cas de perte ou de vol, afin qu'il soit procédé à un blocage ou effacement à distance des données présentes sur le matériel, ainsi qu'à une évaluation de l'impact lié à la perte des données concernées,*
- *protéger les équipements contre les chocs, et les manipuler avec le plus grand soin.*

Les équipes techniques du GSI mettent en œuvre des mécanismes d'administration à distance (blocage, effacement, configuration, etc.) et de journalisation des actions réalisées avec ces équipements notamment lors des connexions à distance.

Article 3.6 – Règles d'utilisation des certificats électroniques

L'utilisation d'un certificat électronique remis à l'utilisateur pour viser ou signer électroniquement les documents, a la même valeur probante qu'une signature manuelle, conformément à sa délégation de signature. À ce titre, un certificat représente personnellement son porteur.

L'ensemble est placé sous l'entière responsabilité de son porteur qui doit en faire un usage strictement professionnel, et prendre toutes les précautions qui s'imposent pour sa sécurité.
En cas de perte ou de vol, l'utilisateur a obligation d'informer dans les plus brefs délais le GSI afin qu'il soit procédé à une demande de radiation du certificat auprès de l'autorité de certification compétente.

Article 3.7 – Droits à l'image

L'image d'une personne ainsi que les enregistrements vidéo et sonores qui se rapportent à elle, ne peuvent être utilisés ou diffusés sans son consentement écrit.

D'une manière générale, les photos, enregistrements vidéo ou sonores que les agents peuvent être amenés à prendre dans l'exercice de leurs fonctions ne doivent donc pas permettre d'identifier directement ou indirectement des personnes physiques.

Pour les photos, l'agent doit s'assurer qu'elles ne permettent pas d'identifier des personnes, des plaques d'immatriculation, des enseignes de magasins étrangères au dossier traité. Il est recommandé de flouter tous ces éléments. Les photos, les enregistrements vidéo ou sonores pris dans le cadre des activités du Sdis 76, ne peuvent pas être utilisés à des fins personnelles, et sont interdits à la diffusion externe sans l'autorisation du service.

ARTICLE 4 – Règles d'utilisation des services Internet

L'accès à Internet et l'exploitation des contenus en ligne sont soumis au strict respect de la législation relative à l'usage des TIC (Technologies de l'Information et de la Communication) : Internet, les réseaux informatiques et les services de communication ne sont pas des zones de non droit.

Le Sdis 76, en fournissant un accès Internet aux agents, doit se conformer à la législation applicable aux fournisseurs d'accès Internet. Les utilisateurs sont avisés que la plupart des sites Internet conservent trace des accès effectués. Ces sites identifient précisément l'identité électronique du visiteur, celle du Sdis 76 en l'occurrence.

En conséquence, sont proscrits et le cas échéant sanctionnés :

- *la consultation ou le téléchargement de données (textes, images, sons) ayant un caractère explicitement indécent, contraire à l'ordre public, portant atteinte à la dignité ou à la vie privée, à caractère injurieux, raciste, pornographique, diffamatoire, en rapport avec une secte ou incitant à la violence (incivilité, terrorisme),*
- *l'usurpation d'identité ou la transgression des autorisations d'accès à internet aggravés par des propos à caractère injurieux, raciste, pornographique ou diffamatoire,*
- *l'émission d'opinions personnelles étrangères à l'activité professionnelle susceptibles de porter préjudice au Sdis 76,*
- *la mise à disposition à des tiers de données et informations confidentielles ou contraires à la législation en vigueur.*

L'utilisateur ne doit pas (liste non exhaustive) :

- *accéder ou tenter d'accéder à un serveur ou à un poste de travail sans avoir été préalablement habilité,*
- *se livrer à des actions portant atteinte à la sécurité et au bon fonctionnement des serveurs, postes de travail et réseau du Sdis 76,*
- *déposer des données professionnelles sur des serveurs grand public ou sur des postes de travail autres que le sien sans en avoir été habilité,*
- *télécharger de la musique, de la vidéo ou tout support numérique n'ayant aucun rapport avec l'exercice de ses fonctions,*
- *activer un service d'échange collaboratif sur Internet (Web Conférence, Call conférence, etc.) sans une autorisation formelle du GSI,*
- *utiliser l'infrastructure du Sdis 76 à des fins de forum de discussion, réseaux sociaux, newsgroup, messageries instantanées n'ayant aucun rapport avec l'exercice de ses fonctions,*
- *participer à des activités rémunératrices, transactions financières (jeux d'argents, paiement en ligne, etc.),*
- *diffuser ou télécharger des données ou des logiciels portant atteintes aux droits d'auteurs ou autres droits de propriété intellectuelle,*
- *consulter ou diffuser des données confidentielles du Sdis 76, des citoyens ou partenaires et de ses collègues, sauf si cela est strictement nécessaire pour la bonne exécution du travail,*
- *consulter ou diffuser des documents et des données protégées par le secret professionnel ou protégées par les dispositions relatives à la vie privée et la protection des données personnelles,*
- *diffuser des messages qui peuvent être considérés comme portant atteinte à la dignité humaine, par exemple: des messages qui pourraient être perçus par le destinataire comme racistes, discriminatoires (sur base du sexe, des préférences sexuelles, de la religion, de l'origine, de la nature du handicap, etc.) ou dégradants,*
- *consulter des sites érotiques, pornographiques ou pédophiles,*
- *participer à des chaînes de lettres/messages,*
- *transférer des messages internes («forwarding»), sans que cela soit professionnellement nécessaire,*
- *rechercher et utiliser des scripts (programmation informatique) et des programmes non connus par le groupement des systèmes d'information du Sdis 76,*

- *créer des pages personnelles sur les ressources informatiques internes ou externes du Sdis 76 en utilisant le système d'information,*
- *créer des messages publicitaires non-sollicités (Spam) depuis les ressources informatiques du Sdis 76,*
- *utiliser la signature professionnelle automatique, l'en-tête/logo ou toute autre indication du Sdis 76 pour des courriers électroniques et des échanges électroniques à des fins personnelles.*

D'une manière générale, l'usage d'Internet est réservé à des fins professionnelles : un usage personnel est toutefois toléré pour autant qu'il ne porte pas atteinte à autrui, au bon fonctionnement du réseau ou à la productivité de l'utilisateur.

Le GSI se réserve le droit de bloquer à tout moment et sans avertissement préalable l'accès aux sites dont il juge le contenu illégal, offensant ou inapproprié. Le Sdis 76 ne saurait être tenue pour responsable de toute infraction commise par un utilisateur ne se conformant pas à ces règles.

ARTICLE 5 – Règles d'utilisation du courrier électronique

Le service met à la disposition des utilisateurs une messagerie électronique pour un usage professionnel.

Un usage privé et raisonnable, dans le cadre des nécessités de la vie courante et familiale est toléré, sous réserve que l'utilisation du courrier électronique n'affecte pas le trafic normal des messages professionnels. **Dans ce cas, l'utilisateur fera apparaître dans le champ objet du message le caractère privatif du message : « PRIVE » ou « PERSONNEL »**

De plus, il devra supprimer dans le corps du message, toute mention relative au Sdis 76 (telle que la signature automatique) et toute autre indication qui pourrait laisser suggérer que le message est rédigé par l'utilisateur dans le cadre de ses fonctions.

En l'absence de toute indication, le message électronique sera considéré comme un message professionnel et non comme un message à caractère privé.

Les règles de conservation des mails :

- *les messages supprimés sont conservés inchangés durant 30 jours sur les serveurs de messagerie,*
- *lorsque le compte d'utilisateur Office 365 est supprimé, les mails sont conservés durant 30 jours à compter de la date de suppression*

ARTICLE 6 – Règles d'utilisation des téléphones

Le Sdis 76 met à la disposition de son personnel des lignes téléphoniques (fixes ou mobiles).
L'utilisateur utilise les moyens de téléphonie mis à disposition à des fins professionnelles. Cependant, un usage raisonné et raisonnable des moyens de téléphonie fixe ou mobile à des fins personnelles est toléré par le service.

ARTICLE 7 – Règles relatives au départ d'un collaborateur du service

Lorsqu'un utilisateur quitte le Sdis 76 (*mutation, fin de contrat, fin d'engagement…*), les accès aux ressources qui lui étaient mises à disposition sont désactivés le jour de son départ. L'utilisateur devra donc anticipé son départ s'il souhaite récupérer des données personnelles stockées sur les outils mis à disposition par le service.

Néanmoins, le service conservera les données pendant un mois avant de procéder à leur destruction. Ainsi, en cas de nécessité et sur accord de la direction générale, un accès sera autorisé aux données.

CHAPITRE 3 – PROTECTION DES INFORMATIONS DU SDIS 76

ARTICLE 8 – Mesures de sécurité informatique

Article 8.1 – Précautions à prendre par l'utilisateur

Afin de permettre la mise en œuvre d'une parade de premier niveau contre les risques liés à l'usage du système d'information du Sdis 76, l'utilisateur doit respecter au minimum les prescriptions évoquées ci-après.

L'utilisateur du système d'information du Sdis 76 doit choisir un mot de passe robuste (*contenant des caractères spéciaux, pas de mots du dictionnaire, pas de prénom ou nom de famille, 8 caractères minimum avec des lettres majuscules et minuscules, des chiffres et des caractères spéciaux, etc.*).

La vigilance est attirée sur les cas suivants et peut conduire à un changement de mot de passe :

- *un utilisateur qui estime que son mot de passe personnel pourrait être connu d'une tierce personne, il est de son devoir de mettre tout en œuvre pour le modifier, soit de son propre chef si cela est possible, soit en contactant le GSI,*
- *les mots de passe personnels, les tags personnels, les badges personnels, ne peuvent jamais être partagés ou révélés à toute autre personne que l'utilisateur concerné ; si cela se produit, l'utilisateur concerné est responsable de toutes les actions entreprises par la tierce partie au moyen de ce mot de passe, tag ou badge,*
- *les identifiants de connexion ne peuvent pas être utilisés par des personnes autres que l'utilisateur qui l'a reçu à titre personnel. Les utilisateurs ne peuvent pas autoriser une autre personne à utiliser leur identifiant de connexion,*
- *l'utilisateur doit protéger spécifiquement les fichiers confidentiels/secrets du Sdis 76 et ne jamais quitter son poste de travail sans verrouiller la session en cours,*
- *l'utilisateur doit mettre en sécurité les supports informatiques (clefs USB, CD-ROM/DVD, cassette, tablette…) contenant des informations confidentielles et doit s'assurer de ne pas exposer toute information sensible transitant par des équipements tels que : fax, imprimantes ou photocopieurs.*

Article 8.2 – Virus Informatiques

Le poste de travail de chaque utilisateur est équipé d'un logiciel anti-virus qui bloque l'accès aux fichiers contaminés et les supprime.
L'utilisateur accordera une vigilance accrue à l'usage des TIC (services internet) et des supports de stockage (clefs USB, CD-ROM, DVD, outils de mobilité (tablettes, smartphones, ..), etc.) : ils favorisent la propagation et/ou l'installation de programmes ou fichiers malveillants susceptibles d'altérer voire de capter les données stockées sur le poste de travail de l'utilisateur à l'insu de ce dernier.
https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

Si l'utilisateur constate des dysfonctionnements inhabituels sur son poste de travail, il devra alerter sans tarder le GSI. Les utilisateurs ne doivent pas essayer de combattre et d'éliminer eux-mêmes les virus sans l'aide d'un membre du groupement des systèmes d'information du Sdis 76.

Afin d'éviter des dégâts ou infections causés par des virus, l'utilisation de logiciels externes, de DVD, de CD ROM, de clés USB ou tous autres médias externes ne peut pas être tolérée sur PC, sur des portables ou sur le réseau (LAN) à moins que ces médias n'aient été au préalable vérifiés par un logiciel anti-virus et par un membre du GSI.

Les utilisateurs ne peuvent pas rédiger, générer, compiler, copier, rechercher, distribuer, lancer ou tenter d'introduire des codes qui ont été conçus pour se reproduire eux-mêmes et pour causer des dégâts ou d'une autre manière gêner le fonctionnement ou l'accès au système, au réseau ou à un composant réseau.

Article 8.3 – Vigilance et obligation de rapport

L'utilisateur doit signaler au responsable du GSI dans les plus brefs délais toute tentative de violation **constatée : sur son poste de travail, sur ses fichiers, sur ses données.** Ceci pour permettre aux services compétents d'adopter les mesures adaptées.

De plus, conformément aux nouvelles directives réglementaires en matière de protection des données à caractère personnel, tout accès illicite, toute perte ou toute fuite de donnée relevant de la loi « informatique et libertés » doit être immédiatement signalée au Délégué à la Protection des Données **(DPD)** qui se chargera d'appliquer la procédure légale adaptée à la situation.

Tout problème ayant trait à la sécurité, toute information concernant les vulnérabilités du système et tout autre sujet relatif à la sécurité informatique doivent immédiatement être rapportés au délégué à la protection des données. Si des agents constatent que d'autres personnes ont pris connaissance de leur mot de passe, ils ont l'obligation d'en informer immédiatement leur supérieur hiérarchique. Ils doivent alors définir un nouveau mot de passe.

Les utilisateurs ne peuvent, en aucun cas, tester les mécanismes de sécurité du Sdis 76 sous peine de se voir sanctionner. Chaque utilisateur veille à la sécurité de ses ressources informatiques. Ainsi, chaque utilisateur interne utilisera des écrans de veille de sécurité et fermera son application en fin de journée.

En règle générale, tout ordinateur qui n'est pas utilisé doit être verrouillé ou arrêté.

Dans le cas où l'utilisateur constate une tentative illicite d'accès à des ressources informatiques depuis son poste de travail verrouillé, il en informe immédiatement le GSI.
Sauf cas exceptionnel, un utilisateur identifié et authentifié dans une application ne peut abandonner son poste de travail sans se déconnecter. Peu importe que ce poste de travail soit ou non équipé d'un mécanisme de protection.

ARTICLE 9 – Contrôles mis en œuvre par le service

La direction du Sdis 76 respecte la vie privée des membres du personnel sur le lieu de travail. Elle exerce toutefois un contrôle de l'usage des moyens de communication et des outils informatiques, dans le respect des dispositions légales applicables.

Article 9.1 – Finalités des contrôles

Les finalités de ce contrôle sont les suivantes:

- la protection des agents de la collectivité dans le cas où une levée de doute est nécessaire concernant un usage illicite par un tiers de [illegible]formations placées sous leur responsabilité,
- la prévention et la répression de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui, ainsi que la répression de ces faits,
- la protection des intérêts du Sdis 76 auxquels sont attachés un caractère de confidentialité ainsi que la lutte contre les pratiques contraires à la sécurité optimale des ressources informatiques et à la disponibilité optimale des réseaux professionnels (limiter l'encombrement),
- la sécurité et/ou le bon fonctionnement technique des systèmes informatiques ainsi que la protection physique des installations,
- le respect de la bonne foi des principes et règles d'utilisation des ressources des systèmes d'information, tels que définis par la présente charte.

Si les données collectées sont traitées en vue de finalités autres que celles pour lesquelles le contrôle a été installé, la Direction générale s'assure que ce traitement est compatible avec les finalités initialement poursuivies et prend toutes les mesures nécessaires pour éviter les erreurs d'interprétation.

Dans le cas où le contrôle mettrait en évidence la bonne foi de l'agent objet d'une suspicion ou d'un acte illicite à son encontre (levée de doute), la collectivité pourra se porter partie civile afin d'apporter son soutien à l'agent auprès des autorités judiciaires.

Dans le cas où le contrôle mettrait en évidence un acte illicite de la part de l'agent ou une infraction de sa part aux règles et directives de la présente charte, la Direction générale appliquera les sanctions selon les dispositifs prévus à l'article 2.

Article 9.2 – Supervision technique

La supervision technique est nécessaire pour assurer le fonctionnement normal du système d'information du Sdis 76. Le GSI contrôle et rejette les flux d'information illicites ou abusifs et éventuellement des pièces jointes aux messages ou des fichiers téléchargés infectés.

Article 9.3 – Contrôle du contenu de l'information

La finalité du contrôle du contenu de l'information s'inscrit dans le cadre des finalités décrites à l'article 9.1.

Conformément aux recommandations émises par la CNIL et à la jurisprudence en vigueur, le Sdis de la Seine-Maritime ne peut accéder qu'aux informations de nature professionnelle, exception faite d'une injonction de justice.

L'administrateur, dans le cadre de ses missions, n'a pas accès au contenu des informations placées sous la responsabilité des agents. Toutefois, si l'autorité judiciaire l'exige ou sur requête du Directeur départemental après avis motivé, l'administrateur peut activer des moyens informatiques lui permettant d'accéder au contenu des informations, en présence de l'utilisateur et/ou d'un représentant du personnel.

La Direction générale est seule destinataire des résultats obtenus lors des contrôles du contenu. Elle prendra les décisions qui s'imposent au regard de ces résultats notamment pour répondre aux requêtes des autorités judiciaires ou pour engager des sanctions ou des actions judiciaires adaptées aux circonstances (que ce soit dans l'intérêt de l'agent ou de la collectivité).

Article 9.4 – Contrôle de l'utilisation d'Internet

Au moyen de logiciels adaptés, le GSI collecte des données générales concernant les sites Internet consultés via le réseau du Sdis 76, y compris des données relatives au contexte de communication et notamment la durée, les protocoles informatiques utilisés, les coordonnées numériques des ressources informatiques concernées et le moment des visites.
Il s'agit d'un contrôle anonyme et non individualisé qui ne vise pas le contenu des informations consultées.
Lorsque, à l'occasion de ce contrôle général le GSI constate une anomalie ou un usage abusif ou illicite, il se réserve le droit de procéder à l'identification d'un utilisateur.
Conformément à la règlementation en vigueur, le GSI réalise une liste générale des sites qui sont visités à partir du réseau informatique du Sdis 76. Cette liste ne fera pas mention de l'identité des visiteurs.
La liste sera régulièrement évaluée. Le GSI peut, sur la base de cette liste, rendre inaccessibles des sites inappropriés en activant les mécanismes techniques de filtrage opérationnel au sein du Sdis 76.

Article 9.5 – Contrôle de l'utilisation du courrier électronique

Sur le principe d'indices généraux tels la fréquence, le nombre et le volume des courriers électroniques, les annexes, etc., certaines mesures de contrôle pourront être prises par le GSI vis-à-vis de ces messages, dans le cadre de la poursuite des finalités décrites à l'article 9.1 ci-dessus.

Article 9.6 – Contrôle de l'utilisation de la téléphonie et des équipements de mobilité

Au moyen de logiciels adaptés, le GSI collecte des données générales concernant les consommations réalisées à partir des systèmes de téléphonie fixe et des matériels de mobilité (téléphone mobile, smartphones, tablettes numériques) du Sdis 76 (numéro appelés, dates, heures et durées des appels).

Il s'agit d'un contrôle anonyme et non individualisé pour les consommations de téléphonie fixe. Il est individualisé pour les consommations réalisées à partir des matériels de mobilité.

Lorsque, à l'occasion de ce contrôle général ou au départ d'autres sources d'information, le GSI constate une anomalie ou un usage abusif ou illicite, il en informe le Directeur départemental qui se réserve le droit, dans le cadre de la poursuite des finalités décrites à l'article 9.1 ci-dessus, de faire procéder à l'identification d'un utilisateur.

Un relevé détaillé des consommations de téléphonie fixe par utilisateur peut être édité en cas d'utilisation abusive. Le détail des consommations (numéro appelé, date, heure, durée) sera alors communiqué au responsable hiérarchique qui donne un avis sur l'opportunité professionnelle des appels après explication de l'agent.

En cas d'abus constaté, la ligne pourra être suspendue ou le matériel mobile repris par le GSI sur demande du supérieur hiérarchique de l'agent ou du Directeur départemental.
En cas de communications abusives, il pourra être procédé à une refacturation auprès de l'utilisateur concerné.

Dans le cas des matériels de mobilité (téléphone mobile, smartphones, tablettes numériques), l'édition de ce relevé détaillé des consommations par utilisateur est systématique. Les données relatives à l'utilisation des services de téléphonie seront conservées conformément aux recommandations de la Commission nationale de l'informatique et des libertés (CNIL).

Article 9.7 – Contrôle individualisé

Le Directeur départemental peut demander au GSI d'individualiser, par des moyens techniques informatiques, les données de contrôle en conformité avec les finalités poursuivies par le contrôle.
Par «individualisation», on entend le traitement des données collectées lors d'un contrôle en vue de les attribuer à un utilisateur identifié ou identifiable.

Le GSI procèdera notamment à une individualisation directe de l'utilisateur s'il suspecte ou a constaté:

- l'accomplissement de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui,
- la violation des intérêts du Sdis 76 auxquels est attaché un caractère de confidentialité,
- une menace à la sécurité et/ou au bon fonctionnement technique des systèmes informatiques ainsi que la protection physique des installations.

Lorsque l'objectif du contrôle tient au respect de la bonne foi des règles et principes d'utilisation des technologies fixées par le Sdis 76, le GSI respectera une phase dite «de sonnette d'alarme» qui vise essentiellement à informer les agents d'une anomalie et les avertir d'une individualisation en cas de récurrence.
Ainsi, si le GSI suspecte ou constate un manquement aux règles et principes de la présente charte et/ou d'autres directives, il avertira l'ensemble des utilisateurs du Sdis 76.
En cas de récidive, le GSI identifiera l'utilisateur auteur du manquement.

L'utilisateur auquel une anomalie d'utilisation des ressources informatiques et/ou des moyens de communication électronique, est attribuée par application de la procédure d'individualisation indirecte décrite ci-dessus, est invité à un entretien, préalablement à l'adoption de toute décision ou évaluation susceptible de l'affecter individuellement.
Par son caractère contradictoire, cet entretien va permettre à l'utilisateur de s'expliquer sur l'utilisation des ressources informatiques et des moyens de communication électroniques mis à sa disposition.

L'utilisateur interne se fera, s'il le souhaite, assister par un représentant du personnel.
Dans le cas où l'usage illicite ou abusif est avéré et où l'utilisateur ne modifie pas son comportement, des sanctions pourraient être envisagées par le Sdis 76.

Article 9.8 – Gestion et contrôle des tiers utilisateurs

Avant qu'une tierce partie (consultant, sous-traitant, etc.) n'obtienne l'accès à une ressource informatique du Sdis 76, une demande doit être formulée auprès du GSI par le pôle qui accueillera la tierce partie. Cette demande précisera la ou les personnes concernées ainsi que la durée d'accès à la ressource informatique. Le GSI procédera à l'examen de la demande et notifiera l'accord du service auprès de la tierce partie et lui définira les termes et conditions d'un tel accès.

De plus, les tiers utilisateurs doivent prendre connaissance et signer la «Charte de Sécurité Informatique et du bon usage des ressources informatiques, électroniques et numériques du Sdis 76 », avant de recevoir une identification de connexion leur permettant d'accéder aux ressources du système d'information du Sdis 76.

Les droits d'accès attribués à un tiers sont limités dans le temps à la seule période nécessaire à l'accomplissement de sa mission. Dans le cas où un prolongement de la durée de la mission est nécessaire, un renouvellement formel des droits d'accès est opéré selon les procédures en vigueur au sein du Sdis 76.

Le GSI se réserve le droit de retirer à n'importe quel moment les privilèges d'un tiers utilisateur notamment lorsqu'il est constaté un non-respect aux principes énoncés dans la présente charte.
Tout comportement d'un tiers utilisateur qui interfère avec le fonctionnement normal et adéquat des systèmes d'information du Sdis 76, qui affecte défavorablement l'utilisation de ces systèmes d'information par les autres utilisateurs ou qui est nuisible ou offensif pour les autres, ne sera ni permis, ni toléré.

Les tiers qui veulent se connecter au réseau du Sdis 76 ou qui veulent transférer des logiciels vers des ordinateurs connectés au réseau informatique du Sdis 76 doivent être informés du règlement antivirus avant d'en recevoir la permission. Une requête doit être faite à l'avance au GSI afin de vérifier, à son arrivée, l'équipement informatique du visiteur.

Si un visiteur refuse de laisser vérifier son équipement informatique pour les virus informatiques, un accord doit être réalisé pour laisser un membre du GSI vérifier son ordinateur en compagnie du visiteur. Toutes les connexions à distance doivent passer par les systèmes de sécurité utilisés pour scanner les virus ou les fichiers attachés non désirés.

Le droit à une connexion entrante par modem ou à une connexion sortante par Internet ne sera pas donné à des tiers utilisateurs à moins que le GSI ne détermine que ces tiers utilisateurs ont un besoin légitime de se connecter de la sorte dans le cadre de leurs activités. Ces privilèges ne peuvent seulement être accordés que par des personnes compétentes en la matière et uniquement pour la période nécessaire à la réalisation des tâches approuvées.

Article 9.9 – Gestion des données de contrôle et droits des utilisateurs

Tout utilisateur peut s'adresser directement au GSI s'il souhaite avoir des informations concernant des données qui sont conservées à son sujet et cela en conformité avec les obligations légales en vigueur notamment en matière de respect du droit d'accès aux données à caractère personnel (RGPD notamment)
Il en est de même si l'utilisateur souhaite faire exercer son droit de rectification ou de suppression de certaines données inexactes à son sujet.

CHAPITRE 4 – INFORMATION DES UTILISATEURS SUR LA GESTION DES SYSTEMES ET DES RESEAUX INFORMATIQUES

ARTICLE 10 – L'Administrateur Système

L'administrateur système, membre du GSI, gère la sécurité des machines connectées au réseau informatique du Sdis 76 ainsi que les serveurs sur lesquels sont installés les différents services mis à la disposition des utilisateurs (service Internet, applications).

L'administrateur système veille à assurer le meilleur service rendu aux utilisateurs dans la limite des moyens alloués. Il lui appartient d'entreprendre toute démarche nécessaire au bon fonctionnement des ressources informatiques dans le cadre des investigations autorisées (cf. article 9) ne contrevenant pas aux dispositions légales relatives à la protection des données privées de l'utilisateur.

L'administrateur système doit informer, autant que possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des ressources informatiques.

L'administrateur système doit, de plus, informer immédiatement le GSI de toute tentative d'intrusion sur le système ou de tout comportement délictueux d'un utilisateur.

L'administrateur système ne doit pas porter atteinte à la vie privée des utilisateurs.

Cette obligation de discrétion concerne aussi bien le contenu de tout message à caractère privé dont les dispositions sont couvertes par le secret des correspondances que de tout fichier à caractère privé dont les dispositions relèvent de la vie privée des utilisateurs.

ARTICLE 11 – Fichier de traces

Toute ressource informatique active génère des suivis d'évènements et a la possibilité de les journaliser dans des fichiers qualifiés de « fichiers de traces ». Ces fichiers sont essentiels à l'administration des systèmes et constituent des aides utiles au diagnostic et à la supervision des ressources informatiques

Ils permettent de remédier aux dysfonctionnements des services rendus par le système d'information ou des ressources informatiques utilisés. Ces fichiers consignent toutes informations comme celles relatives à la messagerie (expéditeur, destinataire(s), date), mais aussi les heures de connexion aux applications de gestion, au service de connexion à distance, numéro de la machine depuis laquelle les services sont utilisés, etc.

Ces fichiers sont destinés à un usage technique. Toutefois, dans le cadre d'une procédure engagée par les autorités judiciaires, le Sdis 76 offrira sa coopération et le cas échéant la transmission des données en fonction des demandes émises par la justice.

La durée de conservation des données de toute navigation internet est d'un an.

Par données de navigation internet, il faut entendre :

- *les informations permettant d'identifier l'utilisateur,*
- *les données relatives aux équipements terminaux de navigation ~~communication~~,*
- *les caractéristiques ainsi que la date, l'horaire et la durée de chaque communication,*
- *les données permettant d'identifier le ou les destinataires de la navigation internet.*

ARTICLE 12 – Logiciels de prise de main à distance

Ces outils permettent d'accéder à distance à l'ensemble des données informatiques de tout poste de travail connecté au réseau informatique du Sdis 76.

Seuls les administrateurs peuvent utiliser ces outils. Il assure la confidentialité des données auxquelles il accède par ce moyen, et s'en tient à la stricte limite de ses besoins. Il doit avant chaque intervention sur un poste, informer et recueillir l'accord de l'utilisateur avant la prise de contrôle du poste de travail.

ARTICLE 13 – Date d'entrée en vigueur et publicité

La présente charte a été soumise pour avis au comité technique le [illegible] juin 2018 et aux représentants du personnel et a été approuvée par le Conseil d'administration lors de sa réunion du 28 juin 2018.

La présente charte est arrêtée par le Président du Conseil d'administration et annexée au Règlement intérieur du Sdis 76. Elle sera publiée au recueil des actes du Sdis 76 et mise à disposition des agents sur l'intranet du Sdis 76.

GLOSSAIRE

Base de données : ensemble d'informations ordonnées présent sur un support informatique associé à des outils automatisés de tri et d'extraction.

CNIL : Commission Nationale Informatique et Libertés. La CNIL est l'autorité administrative indépendante en charge de veiller au respect des dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Compte utilisateur : ensemble de caractères alphanumériques attribué à un utilisateur (user) lui permettant de se connecter à un réseau informatique. Il s'agit d'une série de caractères permettant de décliner son identifiant. L'identifiant est généralement complété par un mot de passe qui sert à authentifier l'agent qui s'est préalablement identifié. Le mot anglais pour identifiant est login.

Confidentialité : qualité d'une ressource informatique de n'être connue que par les personnes autorisées. Respecter la confidentialité des données, c'est garder privées ou secrètes les informations vis à vis des personnes n'ayant pas le droit de les connaître.

Délégué à la protection des données (DPD) : délégué à la protection des données, il est le « chef d'orchestre » de la conformité en matière de protection des données au sein du Sdis. Le DPD est principalement chargé :
- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés,
- de contrôler le respect du règlement et du droit national en matière de protection des données,
- de conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution,
- de coopérer avec la CNIL et d'être le point de contact de celle-ci.

Disponibilité : qualité d'une ressource informatique d'être utilisable à la demande. Ne pas perturber la disponibilité du système, c'est ne pas envoyer de requêtes, de traitements ou d'éditions... qui rendraient les ressources inaccessibles.

Données à caractère personnel : toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Dysfonctionnement : défaillance technique, physique ou logique, rencontrée sur les systèmes, voire les servitudes indispensables à son bon fonctionnement (énergie, climatisation, ...), ainsi que la dégradation des performances ou capacités des systèmes.

Incident de sécurité : fait ou événement, volontaire ou involontaire, issu d'un utilisateur, légitime ou non, voire d'un système externe, et portant atteinte à la sécurité de la ressource administrée, au respect de la loi ou aux intérêts de l'établissement.

Intégrité : qualité d'une ressource informatique de ne pouvoir être altérée, détruite par accident ou malveillance. Respecter l'intégrité des données, c'est ne pas modifier ou détruire des données d'autres utilisateurs sans avoir été autorisé à la faire.

Internet : réseau informatique qui permet à des ordinateurs de communiquer et de partager des données à l'échelle mondiale.

Intranet : réseau informatique réservé à l'usage exclusif d'un organisme.

Intrusion : tentative de prise de contrôle d'un réseau informatique par une personne non habilitée (hacker). Un pare-feu protège en principe le réseau du SDIS de ce type d'attaque, mais une vigilance de chaque utilisateur est la meilleure protection.

Navigation : action de visiter des sites internet à l'aide d'un logiciel spécifique appelé navigateur (en anglais : browser).

Pare-feu : dispositif informatique qui filtre les flux d'informations entre un réseau interne à l'organisme et le réseau externe en vue de neutraliser les tentatives de pénétration en provenance de l'extérieur (en anglais : firewall).

Réseaux sociaux : Ensemble de relations entre des entités sociales. Les réseaux sociaux fournissent des outils qui facilitent le processus de mise en relation autour d'un centre d'intérêt commun et permettent la prise de contact en ligne. Des sites internet permettent à l'internaute de s'y inscrire et d'y créer une carte d'identité virtuelle appelée "profil" plus souvent. Les réseaux sociaux permettent d'échanger avec les autres membres inscrits sur le même réseau, des messages, des vidéos, ou encore des photos. Ils permettent également d'ajouter des "amis" et de gérer ainsi une liste de contacts.

RGPD : Le nouveau règlement européen sur la protection des données à caractère personnel (RGPD) a été adopté par le Parlement européen. Ce règlement a pour objectifs de :

- renforcer la protection des données à caractère personnel traitées et les règles régissant la circulation de ces données ;
- garantir les droits des personnes concernées par les traitements de données ;
- crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données ;
- responsabiliser les acteurs réalisant des traitements de données personnelles, responsables de traitement et sous-traitants compris.

Ressources informatiques : ensemble de moyens informatiques comprenant les réseaux, les équipements (serveurs, poste de travail, baies de stockage, imprimantes, outils de mobilité (Tablettes tactiles, smartphones), synchronisables avec le réseau départemental, certificats électroniques, d'authentification et/ou de signature, etc.), les logiciels, les progiciels, les applications, les bases de données, etc.

Serveur : ordinateur pivot d'un réseau informatique qui héberge un ensemble d'informations communes au réseau (bases de données, fichiers bureautiques, programmes exécutables...).

Site internet : ensemble de pages contenant des informations consultables à l'aide d'un navigateur.

Site internet sécurisé : site internet échangeant des pages encryptées afin de garantir la sécurité des informations transitant entre le site internet et l'utilisateur. Cet encryptage est réalisé au moyen de certificats. Un site sécurisé est en https et un site non sécurisé en http.

Spam (ou courriel non sollicité) : méthode utilisée par des personnes ou des sociétés peu scrupuleuses dont le principe est d'envoyer des messages vers le plus grand nombre de boîtes aux lettres électroniques dans le but de piéger les utilisateurs pour vérifier la validité de l'adresse électronique, d'orienter ceux-ci vers des sites commerciaux la plupart du temps douteux, ou de récupérer des informations personnelles destinées à faire ensuite de la publicité « ciblée »... Certains spams sont destinés à récupérer le numéro de cartes bancaires des internautes pour des utilisations illicites. L'un des objectifs visés par les spammeurs est de constituer des listes d'adresses e-mail valides qui peuvent se vendre dans des milieux commerciaux (sexe, drogue, produits pharmaceutiques,...).
La messagerie des agents du Sdis 76 bénéficie d'une solution anti-spam.

Système d'Information (S.I.): ensemble de ressources matérielles, logicielles, procédurales, organisationnelles et humaines visant à acquérir, gérer, structurer, stocker, traiter, diffuser des informations ou des données sous des formes diverses.

Technologies de l'Information et de la Communication (TIC) : moyens d'échanges, d'informations et de télécommunications (web, messagerie, etc.) mis à dispositions par le Département à partir de serveurs locaux ou à distance constituant les services internet.

Téléchargement : action consistant à enregistrer un fichier informatique sur son propre ordinateur depuis un serveur distant. Le téléchargement peut concerner des logiciels, des formulaires, des documents textuels, de la musique, des vidéos, des films, des photos (en anglais : downloading)

Virus : programme malicieux qui s'installe sur l'ordinateur à l'insu de son utilisateur et qui va effectuer des opérations de nuisance allant de l'utilisation du carnet d'adresses électroniques pour se propager jusqu'à la destruction quasi-totale du contenu du disque dur de l'ordinateur, voire même de la configuration de base rendant la machine totalement inutilisable. Le vecteur principal de propagation des virus est la messagerie électronique et les pièces jointes attachées aux messages, mais il est également possible de voir son PC infecté par la simple navigation sur internet ou l'utilisation de CD- Rom, de provenance peu fiable. Les virus peuvent également se propager par le biais du réseau local de l'établissement : un seul poste infecté par un virus au sein du réseau du Sdis 76 pourrait engendrer une infection généralisée de tous les ordinateurs qui y sont raccordés et paralyser ainsi tous les systèmes en quelques minutes ou quelques heures.