POLE PERFORMANCE ET QUALITE

Charte informatique et libertés

Juin 2017

SDIS 42 LOIRE SAPEURS-POMPIERS

Sommaire

A. Présentation de la charte

a. Finalité et objectifs

Finalité

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.

Objectifs

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

- ✓ assurer la sécurisation des systèmes d'information et de téléphonie du Service départemental d'incendie et de secours (SDIS) 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 au personnel 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 téléphonie mises à disposition des utilisateurs. La sécurité étant l'affaire de tous, chaque utilisateur des moyens informatiques et de téléphonie du SDIS doit y contribuer en mettant en application les règles énoncées dans cette charte. Le SDIS 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.

b. Domaine d'application et définitions

Domaine d'application

La charte s'applique à l'ensemble des personnels (sapeurs-pompiers professionnels, volontaires, personnels administratifs et techniques) et à toutes personnes soumises au règlement intérieur du SDIS, utilisant les moyens informatiques du SDIS, ainsi que ceux auxquels il est possible d'accéder à distance.

Elle précise les sanctions applicables en cas de non-respect de ces règles.

Définitions

Système d'information (SI) et de téléphonie

Le système d'information et de téléphonie du SDIS se compose de :

- ✓ l'ensemble des ordinateurs, fixes ou portables, et tout autre matériel informatique, connectique ou bureautique, tout matériel actif ou passif (serveurs, hubs, câbles du réseau, tout vecteur de communication...), tout moyen de téléphonie (fax, téléphones fixes ou portables...), tout support amovible (PDA, clés USB, disques durs portables…) et tout moyen de reproduction (photocopieurs, scanners...) ; qui seront désignés par le terme « matériel ».

- ✓ l'ensemble des logiciels, systèmes d'exploitation, faisant fonctionner, inter-opérer ou protégeant lesdits ordinateurs et matériels informatiques, et ce compris les protocoles de communication, ainsi que les applicatifs métiers ; qui seront désignés par le terme « logiciel ».

Utilisateur

La présente charte s'applique à toute personne autorisée du système d'information et de téléphonie du SDIS, qui sera désignée par le terme utilisateur. On entend par utilisateur les membres du personnel permanents (agents administratifs et techniques, sapeurs-pompiers professionnels et volontaires) ou temporaires du SDIS (intérimaires, stagiaires…) ainsi que toutes les personnes extérieures amenées à travailler au sein du SDIS et devant utiliser les ressources informatiques et ou de téléphonie.
Pour toute connexion et utilisation du SI depuis l'extérieur (par exemple en télétravail), l'utilisateur est soumis aux termes de cette charte.

Administrateur

Les administrateurs travaillent au sein des bureaux des outils et des systèmes d'information. Ils veillent à la protection, à la maintenance et au bon fonctionnement des systèmes d'informations. Ils respectent la présente charte et s'assurent de son respect par les utilisateurs.
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.

On entend par administrateur 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).

On note que ces interventions se caractérisent par une signature sur les dites ressources au travers d'un profil utilisateur ayant tous les droits de traitement, à savoir le profil dit administrateur.

Référent métier

Les référents métier sont les responsables des logiciels métier. Ils sont soumis aux obligations de confidentialité des administrateurs, au cas où au cours de leur mission, ils viendraient ponctuellement à accéder aux informations personnelles des utilisateurs. Ces référents métier assurent la gestion complète des logiciels métier, à savoir la gestion des droits d'accès, des mots de passe et le fonctionnement des applicatifs de leur ressort. Ils assurent le droit d'accès et de rectification des utilisateurs sur leurs données nominatives détenues par le SDIS au sein de ces fichiers.

Le référent métier est tenu à un devoir de réserve. Il ne peut divulguer les informations auxquelles il a accès de par ses droits de supervision.

c. Contractualisation et responsabilités

Contractualisation

La charte est notifiée à tous les agents (utilisateurs ou administrateurs) par l'intermédiaire d'intranet et elle n'est considérée comme opposable qu'après cette notification.

Dans la mesure où elle détaille certains aspects du dispositif de contrôle de l'usage des ressources, la présente charte a par ailleurs été soumise pour avis aux instances représentatives du personnel du SDIS et pour approbation au bureau du Conseil d'administration du SDIS.

La charte pourra être modifiée pour toute évolution ultérieure en matière informatique ou téléphonique après avis des instances consultatives et approbation du bureau du Conseil d'administration du SDIS. Les modifications seront portées à la connaissance des utilisateurs et des administrateurs via intranet.

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.

… des utilisateurs

Chaque utilisateur utilise les moyens informatiques et de téléphonie auxquels il a accès sous sa propre responsabilité. Il reconnaît 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.

… des administrateurs

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.

B. Les engagements de l'établissement

a. Protection du système d'information

Le SDIS de la Loire s'engage à protéger son système d'information permettant de garantir un haut niveau de sécurité. Pour cela, il est mis en place un compte utilisateur sécurisé, un dispositif anti-intrusion et une sauvegarde périodique des données.

Compte utilisateur

Le droit d'accès d'un utilisateur aux ressources informatiques est soumis à la délivrance par le service informatique d'un compte utilisateur. Ce compte utilisateur, qui se matérialise par un nom d'utilisateur (*login*) et d'un mot de passe personnel, est fourni à tout agent dès son arrivée au SDIS sur demande de son supérieur hiérarchique.

Ce compte utilisateur est personnel, confidentiel et incessible. Il devient automatiquement inaccessible lorsque l'utilisateur quitte le SDIS ou s'il est constaté qu'il a violé l'une des obligations imposées par la présente charte.

Le système de gestion des mots de passe impose une modification périodique des mots de passe, en imposant également un certain niveau de complexité (suite non logique de majuscules, de minuscules, de chiffres et de caractères spéciaux).

Protection anti-intrusion

Le SDIS dispose de pare-feu (*firewall*) pour protéger son réseau. Ces équipements ont pour vocation de limiter certains trafics, soit en fonction des protocoles utilisés soit en fonction des ports, soit en fonction des adresses IP. L'administrateur détermine les règles de filtrage à mettre en œuvre afin de garantir un niveau de sécurité optimal.

Les pare-feu permettent à la fois de vérifier tout le trafic entrant et sortant (messagerie électronique, échange de fichiers, navigation sur internet…) et à la fois d'interdire les sites non autorisés par l'autorité de l'emploi.

Protection contre les atteintes logiques

Les atteintes logiques (virus, chevaux de Troie…) pouvant gravement endommager le réseau informatique et causer des pertes d'informations irrémédiables, le SDIS dispose de logiciels contre les *virus, spyware*, etc… mis en place sur tous les serveurs y compris le serveur de messagerie, ainsi que sur tous les postes utilisateurs.

Sauvegarde des données

Une sauvegarde journalière est programmée par le SDIS. Elle ne concerne que les fichiers enregistrés sur le réseau, ce qui implique que les fichiers stockés en local sur les PC (Disque C) ne sont pas sauvegardés. Tout fichier professionnel doit donc être enregistré et stocké sur le serveur.

Surveillance des connexions

Les services utilisés génèrent, à l'occasion de leur emploi, des « **fichiers de trace** ». Ces fichiers sont essentiels à l'administration des systèmes. Ils servent en effet à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés. Ces fichiers conservent des informations concernant par exemple la messagerie (expéditeur, destinataire, 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, ainsi que les comptes utilisateurs.
Ce type de trace existe aussi pour l'ensemble des services internet et les contrôles portent sur les durées de connexion (de façon globale/par service/par utilisateur), sur les sites visités (de façon globale/par service/par utilisateur) ainsi que sur d'éventuels téléchargements d'images et/ou de textes.

Sur réquisition judiciaire, ces fichiers peuvent être mis à la disposition ou transmis à la justice. De même, les fichiers de trace pourront être utilisés dans le cadre d'une procédure disciplinaire si une utilisation anormale des outils informatiques est avérée. Tout comportement constaté non-conforme à la présente charte pourra entraîner des poursuites internes ainsi que la responsabilité civile et/ou pénale de l'utilisateur selon le cas. La durée de conservation de ces fichiers de trace est de 1 an.

Messagerie

La Direction définit les agents dont la fonction rend nécessaire l'attribution d'une messagerie électronique. L'adresse électronique est composée de : initiale prénom . nom de famille@sdis42.fr. L'adresse électronique peut également être associée à une fonction.

La messagerie doit être utilisée à des fins professionnelles. L'utilisation de la messagerie à des fins personnelles est autorisée par le SDIS à l'exclusion des groupes d'envoi et dans la mesure où celle-ci reste exceptionnelle et n'entrave pas le trafic normal des messages professionnels.

Tout usage illicite ou abusif peut entraîner la suppression immédiate de l'accès à la messagerie.

La taille des messages échangés et le format des pièces jointes sont limités. D'une façon plus générale, des modifications des paramètres de messagerie pourront être faites pour assurer le bon fonctionnement du système d'information du SDIS. Les messages électroniques sont conservés et sont soumis aux procédures de sauvegarde.

Téléphonie

L'ensemble des communications émises ou reçues au moyen des téléphones fixes ou portables du SDIS sont tracées :

- ✓ soit par le biais des autocommutateurs,
- ✓ soit par le biais de factures détaillées remises par les différents opérateurs

b. Déclaration auprès de la Commission nationale de l'informatique et des libertés (CNIL)

Principe

Le SDIS a réalisé l'ensemble des déclarations des fichiers existants comprenant des données nominatives auprès de la CNIL. Dans le cadre de ces déclarations et conformément aux dispositions de la CNIL, le SDIS s'est engagé à ne pas divulguer les informations personnelles communiquées par l'utilisateur sans son autorisation préalable à des tiers.

De plus, et conformément à la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, l'utilisateur bénéficie d'un droit d'accès et de rectification sur l'ensemble des données personnelles détenues par le SDIS.

Si, dans l'accomplissement de son travail ou de ses missions, un utilisateur est amené à constituer des fichiers, il est rappelé que la loi "Informatique et Libertés" impose, préalablement à leur constitution, sous la seule responsabilité de l'utilisateur, que les fichiers comportant un traitement de données nominatives fassent l'objet d'une déclaration auprès de la CNIL.

Numéros de déclaration

Les fichiers de trace ont été déclarés à la CNIL sous le numéro **1112598** (déclaration normale).
Les fichiers de téléphonie et autocommutateurs ont été déclarés à la CNIL sous le numéro **1112590** (déclaration normale).
Le fichier Messagerie a été déclaré à la CNIL sous le numéro **1112591** (déclaration normale).

C. Les droits et obligations des utilisateurs

a. Utilisation du système d'information

Utilisation des données personnelles

L'utilisateur consent à ce que les données à caractère personnel le concernant soient collectées dans le cadre de l'ouverture du compte d'accès. Ces données ne seront utilisées que pour les finalités de cette inscription.

L'utilisateur peut demander au SDIS la communication des informations nominatives le concernant et les faire rectifier en application des dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

L'utilisateur ne peut pas :

- ✓ s'opposer à ce que le SDIS recueille et conserve les informations le concernant et à ce que le SDIS les communique dans le cadre d'une enquête judiciaire,
- ✓ masquer sa véritable identité,
- ✓ altérer, modifier des données ou accéder à des informations appartenant à d'autres utilisateurs du SDIS sans leur autorisation,
- ✓ modifier ou détruire des informations personnelles.

L'utilisateur ne peut accéder qu'aux informations ou fichiers mis publiquement à disposition sur le réseau, ainsi qu'à ses informations ou fichiers personnels.

Accès au système d'information

L'utilisateur doit respecter les obligations suivantes :

- ✓ ne pas communiquer son compte à un autre utilisateur ou toute autre personne,
- ✓ ne pas divulguer son mot de passe et permettre à un autre utilisateur ou un tiers d'accéder à son compte,
- ✓ ne pas utiliser le compte d'un autre utilisateur,
- ✓ ne pas utiliser le système d'information pour des activités professionnelles ou personnelles, incompatibles avec les activités de service,
- ✓ ne jamais quitter un poste de travail sans se déconnecter ou verrouiller son poste. Toute négligence est considérée comme fautive,
- ✓ ne pas laisser un prestataire extérieur se connecter au réseau du SDIS sans surveillance et sans en avertir au préalable le service informatique. Dans ce cas, le prestataire extérieur reste sous l'entière responsabilité dudit utilisateur,
- ✓ signaler auprès du service informatique du SDIS toute tentative de violation de son compte.

Sans préavis et pour des raisons de sécurité, une modification ou une suppression des droits d'accès peut, à tout moment, être décidée par l'administrateur. Le non-respect de ces règles et des obligations légales peut entraîner des poursuites internes ainsi que la responsabilité civile et/ou pénale de l'utilisateur selon le cas.

Utilisation des ressources matérielles et logicielles

L'utilisateur doit respecter les obligations suivantes :

- ✓ prendre soin des ressources informatiques mises à sa disposition par le SDIS,
- ✓ informer l'administrateur de toute anomalie logicielle ou matérielle constatée,
- ✓ n'utiliser les ressources informatiques fournies par le SDIS qu'à un usage professionnel,
- ✓ ne pas effectuer d'opérations pouvant nuire au fonctionnement du réseau et des systèmes informatiques auxquels il accède et à ne provoquer aucune modification, altération ou destruction concernant des données ou fichiers autres que ceux dont il est l'auteur. Toute violation de ces obligations peut engager la responsabilité civile de son auteur et constituer une infraction réprimée par le code pénal,
- ✓ ne pas utiliser ou développer des systèmes parallèles dans le but de contourner l'utilisation d'un logiciel de référence,
- ✓ installer des logiciels, des progiciels ou autres exécutables sur les ressources informatiques du SDIS, sachant que seul l'administrateur est habilité à le faire après validation expresse de la hiérarchie de l'utilisateur,
- ✓ interrompre ou perturber le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau,
- ✓ ne pas chercher à prendre connaissance d'informations ou de fichiers réservés à l'usage d'autres utilisateurs, même dans le cas où ces éléments ne seraient pas protégés par des dispositifs physiques ou logiques,
- ✓ ne pas exploiter d'éventuels failles de sécurité ou anomalies de fonctionnement. Il doit les signaler au service informatique et ne pas en faire la publicité,
- ✓ ne pas désactiver les logiciels antivirus.

Et dans le cas particulier où il est amené à utiliser des matériels portables[1], l'utilisateur doit :

- ✓ sauvegarder les données confidentielles sur des supports sécurisés et ce de manière régulière selon les modalités définies par l'administrateur,
- ✓ ne pas connecter de matériel personnel portable sur le réseau du SDIS sans autorisation expresse et préalable de l'administrateur.

A ce titre, les smartphones mis à disposition par le SDIS sont soumis aux mêmes conditions qu'un PC portable, et régis par les mêmes règles de sécurité (code d'accès, verrouillage automatique, …).

L'utilisation de moyens informatiques, téléphoniques et de communications électroniques personnels à des fins professionnelles doit être déclarée à la hiérarchie, si cette possibilité a été prévue par le SDIS. L'administrateur peut, à sa discrétion, accorder ou révoquer cet usage. L'autorisation sera accordée sous réserve que l'utilisation de ces équipements soit conforme à la charte Informatique.

L'utilisateur peut :

- ✓ créer, à titre exceptionnel, un fichier personnel mais dans ce cas, il s'engage à le stocker sur le disque local de l'ordinateur, dans le répertoire identifié par l'appellation « Dossier personnel », qu'il aura au préalable créé. Le stockage de données personnelles sur tout autre espace de stockage du SDIS est interdit. L'administrateur pourra être amené, pour assurer le bon fonctionnement des ressources informatiques, à supprimer ces fichiers après avoir averti les utilisateurs. L'administrateur s'engage à ne pas prendre connaissance et à ne pas divulguer les informations contenues dans ces dossiers personnels. L'utilisateur est responsable de la sauvegarde de ses données personnelles,

[1] PC, Smartphone, clé USB, CD, disque de sauvegarde…

- ✓ obtenir, auprès de l'administrateur, les informations sur les moyens de contrôle utilisés par le SDIS.

L'utilisateur s'engage formellement à :

- ✓ ne pas importer de fichier ou logiciel de l'extérieur à partir de n'importe quel support[2] dans le système d'information du SDIS sans autorisation préalable et expresse de l'administrateur ;
- ✓ ne pas copier sous quelque support que ce soit des données confidentielles et stratégiques du SDIS, support de travail, dossier de travail sans l'autorisation préalable et expresse de sa hiérarchie ;
- ✓ ne pas transférer (sous quelque forme que ce soit) de données confidentielles du SDIS, support de travail, dossier de travail sans l'autorisation préalable et expresse de sa hiérarchie ;
- ✓ demander l'autorisation expresse de sa hiérarchie avant de diffuser au format numérique tout document engageant le SDIS ou comportant des données stratégiques et ou confidentielles. En cas de doute, il devra se rapprocher de l'administrateur.

[2] Idem 1

b. Utilisation des services internet

Généralités

Les services internet doivent être utilisés à des fins professionnelles. L'utilisation des services internet à des fins personnelles est autorisée par le SDIS dans la mesure où celle-ci reste exceptionnelle et n'entrave pas la navigation des autres utilisateurs.

L'utilisateur doit faire usage des services internet dans le cadre de ses activités professionnelles, dans le respect de principes généraux et des règles propres aux divers sites qui les proposent ainsi que dans le respect de la législation en vigueur.

A ce titre, il est tenu :

- ✓ de ne pas usurper l'identité d'une autre personne et ne pas intercepter de communications entre tiers,
- ✓ de ne pas utiliser ces services pour proposer ou rendre accessible à des tiers des données et informations confidentielles ou contraires à la législation en vigueur,
- ✓ de faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courriel, forums de discussions...
- ✓ de ne pas émettre d'opinions personnelles étrangères à son activité professionnelle ou susceptibles de porter préjudice au SDIS, il se doit un devoir de réserve,
- ✓ de respecter les lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire ou discriminatoire,
- ✓ de ne pas consulter des sites et des pages internet présentant un contenu relevant du droit pénal[3],
- ✓ de ne pas participer à des jeux de hasard, d'argent ou de s'impliquer dans le blanchiment d'argent au moyen d'internet,
- ✓ de réserver l'utilisation de la messagerie à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est autorisée par le SDIS à l'exclusion des groupes d'envoi et dans la mesure où celle-ci reste exceptionnelle et n'entrave pas le trafic normal des messages professionnels. La confidentialité des échanges privés est respectée dès lors qu'une mention précise le caractère privé,
- ✓ de garder une attitude active de communication dans l'usage de sa messagerie et à ce titre, de se connecter régulièrement et de relever sa boîte aux lettres électronique,
- ✓ de veiller à utiliser les réseaux sociaux de façon appropriée. Par exemple : la publication de contenus dénigrant l'établissement, la publication de commentaires diffamatoires contre des collègues ainsi que le partage d'informations confidentielles est prohibé ;
- ✓ de distinguer l'utilisation des services internet faite dans le cadre du service ou dans le cadre personnel,
- ✓ de ne pas diffuser de documents internes à des destinataires internes ou externes qui n'ont pas normalement vocation à en connaître la teneur eu égard à leur qualité ou fonction,
- ✓ de ne pas télécharger et stocker des fichiers réprimés par la loi[4],
- ✓ de ne pas télécharger et stocker des fichiers non professionnels[5].

Respect des droits d'auteurs

En application du code de la propriété intellectuelle, la représentation et la reproduction intégrale ou partielle ainsi que la diffusion d'une œuvre par quelque moyen que ce soit sont soumises à autorisation préalable de l'auteur.
Le téléchargement de logiciels ou d'œuvres protégées, sans autorisation est strictement interdit et peut engager la responsabilité du SDIS et de l'utilisateur.

[3] Pédophilie, pornographie, négationnisme, racisme, incitation à la violence ou à des crimes ou délits, discrimination sexuelle, etc...

[4] Fichiers à caractère pornographique, raciste, négationniste, pédophile, incitants à la violence ou à des crimes ou délits, à la discrimination sexuelle, etc…

[5] Musiques, films, jeux, MP3, MP4, Divx, etc.

Droit à l'image

Dans le respect des règles relatives à la protection de la vie privée et notamment du droit à l'image d'autrui, l'utilisation de toute représentation est soumise à l'autorisation de la personne représentée ou de son représentant légal si elle est mineure.
En aucun cas ces représentations ne peuvent faire l'objet d'activités commerciales et être redistribuées.

L'utilisation de tous services disponibles sur internet, non validés par les administrateurs du SDIS entraîne la seule responsabilité de l'utilisateur. Le SDIS ne peut être responsable de la perte d'information ou du dysfonctionnement du service.

Règles particulières

Messagerie

Chaque utilisateur est responsable du bon fonctionnement de sa messagerie et doit veiller au nettoyage régulier de sa boîte aux lettres.

Par ailleurs, l'utilisateur s'attachera à conserver en local sur son poste de travail (Disque C) les éventuelles correspondances personnelles qu'il serait amené à conserver dans un fichier spécifique portant la mention « Dossier personnel ».

L'utilisation de la messagerie électronique ne doit pas se substituer aux procédures administratives normales, aux circuits administratifs et documents officiels habituellement utilisés.

Les risques d'interception des messages électroniques exigent de limiter l'utilisation de la messagerie électronique à destination de l'extérieur du SDIS aux informations à caractère non confidentiel, non stratégique et non sensible. Si un utilisateur est contraint d'adresser à l'extérieur des informations à caractère confidentiel, stratégique ou sensible, il devra demander une autorisation expresse de sa hiérarchie.

Malgré l'extrême facilité d'utilisation de la messagerie, une attention toute particulière doit être portée à sa rédaction et sa diffusion :

- ✓ l'utilisateur de la messagerie électronique du SDIS doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans ces échanges de courrier que ce soit à titre professionnel ou personnel,
- ✓ l'utilisateur n'émettra pas d'opinion personnelle étrangère ou non à son activité professionnelle susceptible de porter préjudice au SDIS,
- ✓ l'utilisateur ne perturbera pas les autres utilisateurs par l'utilisation abusive du courrier,
- ✓ l'utilisateur ne portera pas atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants.

Le message électronique est un écrit pouvant engager le SDIS. Tout utilisateur s'engage à ne pas envoyer à d'autres utilisateurs ou à tout tiers extérieur au SDIS des messages comportant une atteinte à la personnalité d'autrui, contenant des propos injurieux, racistes, de nature politique, contre la bienséance, pouvant porter atteinte au SDIS ou à toute personne et de manière plus général tout message contraire à la loi.

Toute utilisation imprudente de la messagerie peut nuire directement ou bien indirectement aux intérêts du SDIS et engagera la responsabilité personnelle de son auteur.

Pour assurer le bon fonctionnement de ses services et en assurer la sécurité, l'administrateur se réserve le droit de mettre en œuvre toute solution technique permettant la mise en quarantaine des messages contenant des virus et le rejet des messages véhiculant des informations non désirées (communément nommés SPAMS). La mise en œuvre de telles solutions donnera lieu à une information de l'utilisateur, conformément aux dispositions légales en vigueur.

Réseaux sociaux

Les règles spécifiques à l'utilisation des réseaux sociaux sont contenues dans le guide des bons usages des médias sociaux. Celui-ci est consultable, comme tous les documents structurants, par le biais d'intranet.

Internet

Les personnels du SDIS, pour accéder à internet dans les enceintes du SDIS, peuvent être amenés à utiliser des ressources informatiques non proposées et non administrées par le SDIS (ADSL des amicales, accès via réseaux mobiles...). Le SDIS n'est pas responsable de ces accès à internet. Les utilisations qui peuvent en être faites n'engagent en aucune manière le SDIS.

Concernant les sites internet sécurisés, le SDIS se laisse la possibilité, via ses équipements de sécurité, de décrypter les échanges informatiques transitant. Dans ce cas, l'utilisateur est informé de ce point avant toute consultation.

Il est demandé aux personnels du SDIS de respecter l'ensemble des droits et des obligations incombant aux sapeurs-pompiers et aux agents publics ainsi que de ne pas porter atteinte à l'image du SDIS.

Toute personne s'engage à respecter l'éthique du réseau internet. Il est notamment rappelé que se faire passer pour une autre personne, envoyer un message anonyme, utiliser une adresse IP non autorisée sont interdits.
Il est aussi formellement interdit de se connecter ou de visiter des sites pornographiques, racistes, négationnistes, pédophiles et de manière plus générale tout site portant atteinte aux bonnes mœurs.

L'utilisation des boîtes aux lettres personnelles via internet, la participation à des forums sont tolérées à titre personnel, et tout abus pourra être sanctionné. De même, les services Webmail (Hotmail, Yahoo, Free…), et les messageries instantanées (ICQ, AIM, MSN MESSENGER …) sont à utiliser à des fins professionnelles et après autorisation de la Direction. Toutefois, leurs utilisations à titre personnel sont tolérées, et tout abus pourra être sanctionné.

L'usage d'un quelconque moyen personnel pour se connecter au réseau internet est strictement interdit et sera considéré comme une faute.

L'utilisateur s'engage à respecter les dispositions législatives et réglementaires en vigueur, notamment celles relatives à la propriété littéraire et artistique, contenues, en particulier, dans le code de la propriété intellectuelle. Le téléchargement de logiciels ou d'œuvres protégés, sans autorisation des ayant-droits engage la seule responsabilité de l'utilisateur. L'administrateur se réserve la possibilité d'effacer du système d'information toute copie de ces logiciels et œuvres protégés.

c. Téléphonie

Le SDIS met à disposition de son personnel des moyens de téléphonie fixes et/ou mobiles dans le cadre de leur mission professionnelle. Ces moyens de téléphonie doivent être utilisés à des fins professionnelles. Une utilisation à des fins personnelles est autorisée par le SDIS dans la mesure où celle-ci reste exceptionnelle.
Tout usage abusif des moyens de téléphonie à des fins personnelles pourra donner lieu à des sanctions.

Chaque utilisateur s'engage à prendre soin des ressources de téléphonie mises à sa disposition par le SDIS. Il doit informer l'administrateur de toute anomalie constatée.

De plus, l'utilisateur des moyens de téléphonie mis à disposition par le SDIS s'interdit :

- ✓ de masquer sa véritable identité,
- ✓ de porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité,
- ✓ d'interrompre ou de perturber le fonctionnement normal du réseau téléphonique,
- ✓ d'avoir des propos comportant une atteinte à la personnalité d'autrui, contenant des propos injurieux, racistes, négationnistes, pornographiques, diffamatoires, de nature politique et de manière plus générale contraires à la Loi.

Le SDIS ne pourra être tenu responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se serait pas conformé à ces règles et à l'ensemble des obligations légales. Le non-respect de ces règles et des obligations légales peut entraîner des poursuites internes ainsi que la responsabilité civile et/ou pénale de l'utilisateur selon le cas.

Dans un souci de maîtrise des dépenses liées à l'utilisation des services de téléphonie du SDIS, l'intégralité des communications peuvent faire l'objet d'un contrôle de gestion. Tout abus constaté du personnel à des fins non professionnelles et établi de manière contradictoire pourra être sanctionné. De même, toute consommation non justifiée dans le cadre professionnel pourra faire l'objet de refacturation. Il appartiendra dans ce cas au SDIS d'établir des justificatifs.

La mise en œuvre de telles solutions est réalisée conformément aux dispositions légales en vigueur.

D. Les obligations des administrateurs

a. Rôle et missions

Les règles de déontologie et de sécurité applicables aux administrateurs sont justifiées par le rôle de confiance et les responsabilités qui leurs sont confiés.

Rôle

Par la nature même de ses missions, l'administrateur bénéficie d'une position technique qui lui permet d'avoir accès :

- ✓ aux équipements/ressources placés sous sa responsabilité (domaine plus ou moins étendu),
- ✓ aux données techniques générées ou utilisées par les ressources (ex : journaux systèmes),
- ✓ aux informations relatives aux utilisateurs[6], y compris celles qui pourraient être stockées sur le disque dur du poste de travail.

En outre, afin de conduire les actions quotidiennes afférentes à sa mission, l'administrateur est doté de droit d'accès privilégiés sur les ressources à sa charge. Les risques associés à ces droits d'accès privilégiés peuvent être :

- ✓ l'accès à des informations dont il n'est pas destinataire, certaines revêtant un caractère sensible telles que des données à caractère personnel ou relevant de la vie privée des agents, utilisateurs, ou administrés,
- ✓ la réalisation d'actions potentiellement dangereuses pour la sécurité des SI du SDIS : modification ou contournement de mécanismes de protection, la création ou la modification de comptes utilisateurs, la destruction ou la modification de fichiers…

Ces différents risques justifient les principes et règles définis dans les sections à suivre et représentant le socle de base de la réflexion et de l'action responsable des administrateurs.

Missions

Administration et exploitation des ressources

En application des consignes formelles qui leur ont été transmises et dans le cadre des procédures internes préalablement définies, les administrateurs sont chargés de la mise en production, l'administration et l'exploitation des systèmes informatiques et de télécommunications de l'établissement et ont le devoir d'assurer le bon fonctionnement et l'optimisation des ressources placées sous leur responsabilité, ci-après leur « périmètre technique respectif ».

A ce titre, ils peuvent en particulier :

- ✓ appliquer les mesures permanentes ou provisoires en vue d'améliorer les performances des ressources ou le confort d'utilisation et en assurer la maintenance, le support et l'évolution,
- ✓ assurer la sauvegarde des données hébergées ou générées par les ressources et plus généralement la gestion des données professionnelles les empruntant, conformément notamment aux besoins exprimés en matière de continuité des services du SDIS.

[6] Données Métier, historique des connexions internet, profil d'habilitation ainsi que les messageries et leur contenu

Sécurisation et contrôle des ressources

Les administrateurs ont également la charge de la sécurité et de la surveillance des ressources placées sous leur périmètre technique respectif.

A ce titre, en application des consignes propres aux ressources concernées et dans le cadre de leur fiche de poste et des procédures internes préalablement définies, ils peuvent en particulier avoir à :

- ✓ traiter (détection, analyse, éradication, filtrage, etc.) tout flux informatique présentant des risques de sécurité [7] ou fonctionnellement atypiques,
- ✓ procéder à des vérifications techniques sur les fichiers et bases de données, la messagerie, les connexions à internet, les fichiers de journalisation…, afin de déceler tout dysfonctionnement ou incident de sécurité qui pourrait porter atteinte au bon fonctionnement et à la sécurité du SI,
- ✓ réaliser une supervision permanente des performances et capacité des systèmes et une analyse régulière des données générées par ceux-ci afin de conférer disponibilité, intégrité et confidentialité aux données,
- ✓ isoler, arrêter ou reconfigurer des comptes utilisateurs, des équipements ou des applications informatiques pouvant compromettre la sécurité d'ensemble du SI,
- ✓ préserver les traces et tous les éléments techniques nécessaires à la résolution du dysfonctionnement ou de l'incident de sécurité et à toute investigation ultérieure, dans le respect de consignes préalablement définies.

D'une manière générale, l'administrateur prend toutes mesures utiles afin d'empêcher toute tentative d'intrusion sur les SI, et tout comportement malveillant ou à risque pouvant entraîner des dégradations du bon fonctionnement du réseau, la mise en jeu de la sécurité, la destruction ou l'altération des données informatiques, la mise en danger de l'intégrité des systèmes informatiques et susceptibles de causer un préjudice au SDIS ou à un tiers.

Pour assurer l'ensemble de leurs missions, les administrateurs sont formés aux tâches et responsabilités qui sont les leurs, ainsi qu'aux procédures et composants techniques qu'ils gèrent, et sont sensibilisés aux éléments juridiques encadrant leur exercice professionnel au sein du SDIS.

7 Virus, intrusion, utilisation d'un logiciel interdit, etc…

b. Obligations

Obligations d'ordre général

Utilisation modérée du compte administrateur

Les droits d'accès privilégiés d'un administrateur sont justifiés par le besoin inhérent à ses activités sur les systèmes. Ainsi, il est interdit à l'administrateur de faire usage de ces droits à d'autres fins que celles de ses missions et dans les limites de son périmètre technique.

De plus, dans le cadre de leurs fonctions, tous les administrateurs utilisent un compte individuel, pourvu de privilèges d'administration et permettant l'imputabilité nominative de leurs actions sur les ressources. En cas de besoin de créer un compte générique ou fonctionnel (ex : compte de service), le responsable hiérarchique ou fonctionnel valide obligatoirement le bien-fondé de cette demande et définit les limites de l'autorisation ainsi délivrée. Dans tous les cas, il est strictement interdit d'utiliser ce compte pour réaliser des actions non prévues expressément par l'autorisation délivrée.
Enfin, lorsque l'utilisation de droits particuliers n'est pas nécessaire, l'administrateur s'identifie sur le système d'information avec un profil utilisateur. Il reste à tout moment soumis au respect des règles définies dans la charte informatique et liberté du SDIS.

Préservation de la confidentialité des données consultables ou consultées

Lorsqu'ils ne sont pas des fonctionnaires soumis par ailleurs au secret professionnel dans le cadre des règles instituées dans le code pénal, les administrateurs sont tenus à un devoir de discrétion professionnelle pour toutes les données, informations ou documents dont ils ont connaissance dans l'exercice de leurs fonctions, qu'elles concernent les agents du SDIS ou les usagers.

Les administrateurs observent en particulier le secret ou l'obligation de confidentialité qui protège spécifiquement certaines catégories de données, en particulier les données nominatives ou qui intéressent de manière évidente la vie privée des usagers et des utilisateurs (ci-après désignées comme les données privées), et ce y compris les messages et tous les fichiers signalés ou se révélant comme privés qui sont couverts par le secret des correspondances ou bénéficiant du droit au respect de la vie privée. Les administrateurs sont tenus d'alerter le chef du groupement des nouvelles technologies de l'information (GNTI) qui fait office de correspondant informatique et liberté en cas de doute ou s'ils constatent un dysfonctionnement sur le traitement de données nominatives.

Concernant les données dites privées, et sauf disposition législative particulière en ce sens (ex. obligation de dénonciation de crimes ou délits ou cas de requête judiciaire), les administrateurs ne peuvent en aucun cas, y compris à l'égard des échelons hiérarchiques supérieurs, être contraints de divulguer des informations protégées qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions.
S'agissant par ailleurs d'informations issues de traitements de données à caractère personnel au sens de la loi dite Informatique et Libertés, il est rappelé à l'administrateur que ces données sont couvertes par une obligation légale de sécurité et de confidentialité et qu'il convient de prendre à leur égard toute mesure de nature à empêcher qu'elles ne soient communiquées à des personnes non autorisées.
A cet égard, en cas de demande d'accès ou de communication d'informations adressée directement à l'administrateur portant sur des traitements de données à caractère personnel, l'administrateur procède au préalable à la vérification de la qualité du demandeur en tant que destinataire ou tiers autorisé auprès soit du responsable fonctionnel du traitement soit du chef du GNTI, correspondant Informatique et Libertés.

Pour remplir sa mission de surveillance des ressources, sans violer les droits des utilisateurs, l'administrateur veille en premier lieu à opérer un contrôle répondant aux principes généraux de nécessité et de finalité tels que prévus par la Loi.

Ainsi, suivant ces principes, l'administrateur se doit d'utiliser les moyens (bases de données, journaux, traitements, sauvegardes, ...) permettant de remplir sa mission sans aller au-delà du but recherché et en respectant les objectifs stricts du contrôle opéré. L'administrateur a donc l'obligation de toujours proportionner ses actions et de n'accéder qu'aux données nécessaires à l'accomplissement de ses missions. Sa démarche doit être toujours motivée par des impératifs de sécurité ou de continuité des applications métiers.

De surcroît, aucune exploitation des informations dont l'administrateur peut avoir connaissance dans l'exercice de ses actions de contrôle ne saurait être opérée, d'initiative ou sur ordre hiérarchique, à des fins autres que celles spécifiées dans le cadre des formalités préalables auprès de la CNIL et liées au bon fonctionnement et à la sécurité des ressources comprises dans son périmètre technique respectif.

Respect des utilisateurs

Les activités des administrateurs sur les systèmes d'information servent en priorité à la mise en œuvre, au maintien voire à l'amélioration de la qualité et de la continuité des services rendus à l'utilisateur.

Ainsi, lorsque l'intervention de l'administrateur peut avoir une influence sur le service rendu par un système, il doit intégrer au maximum les contraintes opérationnelles et avertir les utilisateurs, par le moyen le plus approprié (note d'information, intranet, courrier électronique, téléphone,...), avec un préavis et une information suffisante (conséquences, date et heure de début et de fin prévue de l'intervention).

Dans tous les cas, l'administrateur qui doit interrompre tout ou partie du service rendu aux utilisateurs doit :

- ✓ limiter la gêne occasionnée en réduisant autant que possible la durée et la fréquence de ces interruptions et en choisissant des plages horaires adaptées,
- ✓ indiquer aux utilisateurs les moyens concrets de supporter ces perturbations s'il y en a,
- ✓ accuser réception que l'information envoyée a été prise en compte.

Dans le cas particulier de l'utilisation de logiciels de télémaintenance qui permettent de détecter et réparer les pannes à distance ou de prendre le contrôle à distance du poste de travail d'un utilisateur, toute précaution doit être prise afin de garantir la transparence de l'emploi de ces outils.

En particulier l'administrateur doit :

- ✓ avant toute intervention, informer et recueillir préalablement l'accord de l'utilisateur pour pouvoir prendre la main sur son poste (l'accord peut être donné par oral ou par simple validation d'un message d'information apparaissant sur son écran),
- ✓ assurer la traçabilité des opérations de maintenance (par exemple, par la tenue d'un registre des interventions),
- ✓ accéder aux seules données nécessaires à l'accomplissement de sa mission.

Enfin, dans les cas de mobilité (interne comme externe) d'un utilisateur, les administrateurs mandatés, veillent et contribuent à la fermeture technique des comptes informatiques de l'utilisateur et à la destruction de ses données personnelles à compter de son départ. Si besoin, ils remettent à son successeur toutes les données électroniques (fichiers, messages...) nécessaires à la continuité de sa mission.

A défaut de mise en œuvre de ces consignes préalablement au départ de son poste, l'utilisateur est informé que, eu égard à la destination professionnelle des outils et en raison de considérations liées à l'optimisation des ressources, les administrateurs sont autorisés après son départ à procéder à l'effacement ou transmission des données concernées au regard de leur contexte.

Sécurisation des informations

Les administrateurs observent strictement les règles de sécurité et les limites fixées à leurs interventions, notamment :

- ✓ ils appliquent les mesures de sécurité définies par le SDIS ;
- ✓ ils observent les règles de sécurité en vigueur visant à protéger l'utilisation des droits d'accès privilégiés qui leur sont attribués. A cet égard, ils veillent particulièrement à la protection des postes de travail à partir desquels ils exercent leurs fonctions et sécurisent les identifiants et authentifications des comptes d'accès privilégiés conformément aux règles de l'art ;
- ✓ ils ne modifient les configurations et les droits d'accès aux ressources que dans le respect des procédures d'administration et d'exploitation préalablement définies ;
- ✓ ils ne prennent pas leurs consignes d'une personne non habilitée pour des recherches d'informations de connexions par exemple, (quel que soit son niveau hiérarchique) et se réfèrent à leur responsable hiérarchique ou fonctionnel pour toute requête leur paraissant inappropriée.

En tout état de cause, les administrateurs ne contournent pas les procédures de sécurité établies et, en particulier, ils ne désactivent pas de leur propre initiative les mécanismes de traçabilité ni ne portent atteinte à l'intégrité des fichiers de journalisation qui permettent de définir les actions qui leur sont imputables.

Tout constat de contournement de cette règle serait constitutif d'une faute grave.

Obligations spécifiques aux opérations de contrôle

Respect des données personnelles

Comme indiqué précédemment, il est dans la fonction d'un administrateur d'assurer le fonctionnement normal des ressources dont il a la charge ainsi que leur sécurité, ce qui entraîne, entre autres, qu'il ait accès à des informations relatives aux administrés ou agents. Toutefois, dans le cadre des activités de contrôle opérées, cet accès technique aux données n'emporte pas nécessairement le droit pour l'administrateur de les divulguer.

A cet égard, suivant les principes qui sont posés dans la charte informatique et liberté du SDIS, l'administrateur est conduit à distinguer deux catégories de données :

- ✓ les données présumées à caractère professionnel (toutes données à l'exclusion de celles visées dans la catégorie à suivre) ;
- ✓ les données, dossiers, fichiers, répertoires, archives ou messages identifiés par l'utilisateur comme privé, conformément à la convention de nommage indiquée par la charte précitée.

Ainsi, en présence de données bénéficiant de la présomption de caractère professionnel, l'administrateur peut opérer et reporter, à tout moment et hors la présence des utilisateurs, toute opération de contrôle nécessaire au bon fonctionnement et à la sécurité des SI ou sollicitée dans le cadre de la gestion d'un incident constaté.
Par contre, l'administrateur qui, dans le cadre d'une opération de contrôle, se trouve en présence de contenus relevant de la seconde catégorie, respecte les prescriptions fixées par la jurisprudence, qui exigent :

a) soit la présence de l'utilisateur : celle-ci est alors notifiée dans le rapport d'incident, lui-même approuvé par l'utilisateur à l'issue du contrôle par tout moyen approprié, et le cas échéant accompagné de réserves émises par l'utilisateur,

b) soit, à défaut de la présence de l'utilisateur, que celui-ci ait été dûment contacté par l'administrateur ou sa hiérarchie pour l'inviter à être présent, par tous moyens appropriés et notifiés dans le cadre du rapport d'incident, et que le SDIS puisse justifier d'un cas de force majeure c'est-à-dire d'un risque ou événement particulier portant atteinte à la sécurité de son SI et présentant à la fois un caractère d'urgence et de gravité certain. L'ensemble des éléments de preuve attestant de cette situation particulièrement motivée sont alors consignés dans le rapport d'incident établi par l'administrateur, qui le transmet pour validation au chef du GNTI.

Remarque : dans les cas a) et b), la présence comme l'information préalable de l'utilisateur n'implique pas nécessairement l'accord de ce dernier.

En cas d'accès à des données se rapportant de manière évidente à la vie privée d'un utilisateur mais non signalées comme telles par l'intéressé, aucune faute ne peut être retenue à l'encontre de l'employeur ni de l'administrateur en charge des opérations de contrôle. Dans ce cas, sauf l'obligation particulière de dénonciation de crimes ou délits applicable aux fonctionnaires ou le cadre d'une requête judiciaire, l'administrateur applique le droit au respect de la vie privée de l'utilisateur conformément aux principes généraux dégagés dans la présente charte.

Rapidité de traitement des incidents de sécurité et poursuites éventuelles

Dans le cadre de leurs fonctions, les administrateurs peuvent être alertés sur des dysfonctionnements ou des incidents de sécurité touchant les SI. Comme indiqué dans le glossaire annexé :

- ✓ les dysfonctionnements regroupent toutes les défaillances physiques ou logiques rencontrées sur un système, voire sur les servitudes indispensables à son bon fonctionnement (énergie, climatisation...), ainsi que la dégradation des performances ou capacités des systèmes,
- ✓ les incidents de sécurité regroupent tous les faits ou événements volontaires ou involontaires, issus d'un utilisateur légitime ou non, voire d'un système externe, et portant atteinte à la sécurité du système administré, au respect de la loi ou aux intérêts du SDIS.

Un administrateur constatant un dysfonctionnement réagit selon les consignes propres au système concerné et prend immédiatement les mesures permettant de :

- ✓ faire cesser la défaillance (ainsi que ses éventuels effets ultérieurs) en cohérence avec le besoin opérationnel qui reste prioritaire,
- ✓ recouvrer le niveau nominal de fonctionnement et de sécurité du système,
- ✓ assurer la continuité de service, au besoin en mode dégradé.

Dans le cas du constat d'un incident de sécurité, l'administrateur établit un rapport d'incident qui est communiqué sans délai au chef du GNTI qui, suivant la nature des faits rapportés et les suites envisagées, peut demander à l'administrateur d'identifier nommément le ou les utilisateur(s) concerné(s).

Lorsque des données privées sont concernées par le rapport d'incident, l'administrateur s'attache alors à spécifier uniquement leur caractère présumé illicite ou abusif sans en révéler le contenu.
Un rapport d'incident peut, le cas échéant être suivi :

- ✓ soit d'une simple mise en garde de(s) l'utilisateur(s) concerné(s) par le chef du GNTI ou le responsable hiérarchique (par exemple, rappel des dispositions de la charte informatique et liberté),
- ✓ soit, en raison de la gravité des faits ou de la violation répétée des règles internes précisées notamment dans la charte informatique et liberté du SDIS, être signalé par le chef du GNTI auprès du chef du bureau des ressources humaines qui décide, en concertation avec le Directeur départemental des services d'incendie et de secours (DDSIS), de la suite portée au dossier.

Cette décision peut conduire notamment à :

a) **un dépôt de plainte** : cette situation s'applique en particulier dans le cas de crimes ou délits constatés entrant en particulier dans le domaine du manifestement illicite à savoir, tel que défini par la jurisprudence : atteintes aux mineurs (pornographie enfantine), incitation à la haine ou la violence raciale, atteintes à la dignité humaine, apologie de crimes de guerres ou de crimes contre l'humanité, contenus racistes, antisémites, négationnistes ou révisionnistes.
Dans ce cas, le DDSIS, auteur de la mesure de dépôt de plainte, valide et transmet à l'administrateur les requêtes officielles l'obligeant en particulier à remettre à l'autorité judiciaire (magistrat ou officier de police judiciaire destinataire de la requête) toute information susceptible d'intéresser l'enquête, et ce compris les données privées de l'utilisateur,

b) **des investigations techniques complémentaires** : ces investigations ont pour seul objet de conforter la qualification des faits constatés et la nature ou le niveau des mesures et sanctions appropriées.
Dans ce cas, le chef du bureau des ressources humaines ou le DDSIS sont seuls habilités à solliciter le chef du GNTI afin que l'administrateur, auteur du rapport d'incident initial, procède à une investigation ciblée plus approfondie sur les sessions de travail et, dans les limites définies précédemment, sur les données se rapportant ou appartenant à cet (ces) utilisateur(s). Comme pour tous les incidents pouvant déboucher sur des poursuites disciplinaires ou judiciaires, toutes les mesures adaptées afin de préserver les éléments de preuve des faits constatés doivent alors être prises. Eu égard à cette exigence, le chef du GNTI peut décider, suivant la nature des enjeux et la complexité des procédures et systèmes concernés, de confier la responsabilité de la collecte des éléments de preuve à un tiers compétent offrant par ailleurs des garanties d'impartialité et de neutralité de son action.

En toute hypothèse, l'administrateur et les différents responsables impliqués dans la procédure de gestion des incidents de sécurité agissent avec la plus grande discrétion et respectent à tout moment le principe de présomption d'innocence.

Préservation des preuves

La preuve est la démonstration de la réalité d'un fait, d'un état, d'une circonstance ou d'une obligation. Elle a pour finalité soit d'apporter des éléments contradictoires aux faits reprochés, soit d'affirmer les allégations et ainsi d'aider le juge à se forger une intime conviction ou le commandement à apprécier l'opportunité d'une éventuelle sanction ou action en justice.

Pour fixer la preuve dans le temps et éviter sa disparition ou son altération, l'administrateur respecte les précautions conformes aux règles de l'art en matière de sécurité et d'investigation informatique légale.
Ainsi, lorsqu'il intervient en particulier dans le cadre d'un incident de sécurité en cours d'instruction, l'administrateur doit agir rapidement afin de :

- ✓ déconnecter, en cohérence avec les besoins opérationnels, le serveur, l'élément de stockage ou le poste client du réseau afin d'éviter toute action d'effacement ou de modification de preuve postérieure à la découverte du délit,
- ✓ éviter, dans la mesure du possible, d'éteindre l'équipement incriminé (cette opération pouvant causer l'effacement des traces présentes en mémoire) ; si la machine doit cependant être éteinte, le choix de la méthode d'extinction du système (débranchement du cordon d'alimentation ou procédure ordinaire d'arrêt système) s'opérera suivant les paramètres suivants : l'ordre de volatilité des informations, leur priorité dans les investigations et l'impact des opérations sur les données ciblées,
- ✓ ne pas connecter de supports amovibles (ce qui générerait des traces perturbatrices dans les journaux),
- ✓ restreindre l'accès physique et logique à la ressource incriminée de manière à ce que personne ne modifie sa configuration avant l'intervention des services compétents,

- ✓ le cas échéant, verrouiller le(s) compte(s) du (des) utilisateur(s) mis en cause, ainsi que l'accès aux comptes de messagerie et en informer les personnes concernées,
- ✓ dans tous les cas (y inclus celui des investigations techniques complémentaires précédemment visées), l'administrateur assure une traçabilité et un historique de son intervention. A ce titre, il documente dans un cahier des opérations (journal de bord) l'ensemble des constatations faites et des actions effectuées tant sur les systèmes que sur les données, en précisant notamment :
  - les dates et heures (heure système du poste et heure GMT réelle),
  - le nom des fichiers ou commandes exécutés ainsi que les login et mot de passe utilisés si des actions d'administration sont nécessaires.

Enfin, d'une manière générale, l'administrateur assure l'intégrité des données collectées et préserve le plus grand nombre d'informations pertinentes pouvant compléter et appuyer ses constatations telles que : les supports de sauvegardes récentes et les journaux d'évènements.

Le Président du conseil d'administration
du service départemental
d'incendie et de secours de la Loire

Bernard PHILIBERT

Glossaire

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.

Utilisateur : personne ou groupe de personnes ayant reçu l'autorisation d'accès aux ressources informatiques et de communication de l'établissement. Sont concernées toutes les personnes quel que soit leur positionnement dans l'établissement (élu, fonctionnaire, contractuel, vacataire, stagiaire d'école, personnel temporaire, partenaire extérieur intervenant ponctuellement, sapeur-pompier volontaire, volontaire service civique,...).

Administrateur : personne chargée de la maintenance et du suivi (gestion de la configuration, gestion des pannes, gestion de la sécurité, gestion des performances) pour un site, un serveur, une application...

Système d'information (SI) : ensemble des moyens de production et de traitement (serveurs, postes de travail et autres périphériques informatiques), de stockage que constituent tous les supports magnétiques fixes ou amovibles (CD Rom, clé USB...), de duplication permettant la reproduction d'un document ou d'une information originale (ex : photocopieuses, scanners,...), de communication tels que les réseaux informatiques (messagerie, internet) et téléphoniques.

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

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.

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.

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.

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.

Logiciel espion ou spywares : codes malicieux qui viennent infecter les ordinateurs lors de l'installation de programmes supposés sûrs (la plupart du temps des logiciels gratuits diffusés sur internet) mais qui ont comme fonction cachée de mettre en place des « portes dérobées » sur les ordinateurs destinées à capter des informations personnelles sur les utilisateurs (habitudes de navigation sur le web, adresse e. mail, n° de cartes bancaires,...), dans le but d'en faire une utilisation commerciale peu scrupuleuse ou à toute autre fin potentiellement clandestine. Dans la plupart des cas, la désinstallation du programme infectant ne désinstalle pas les logiciels espions qui restent actifs.

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).

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.

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

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 bénéficie d'une solution anti-spam.

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 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.

Donnée à caractère personnel : toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

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.

Table des matières