Charte informatique DU SDIS DE LA MEUSE

La présente charte a pour objet de définir les règles d'utilisation des moyens et systèmes informatiques de la Direction des Services d'Incendie et de Secours de la Meuse.

CHAMP D'APPLICATION :

Les règles et obligations de la présente charte s'appliquent à toute personne : employé(e), collaborateur (SPV) et plus généralement à toute personne (stagiaire….) autorisée à utiliser les moyens et systèmes informatiques de l'ensemble des sites de l'établissement (direction, centre de secours…).

RESPECT DES RÈGLES DE DÉONTOLOGIE INFORMATIQUE :

Chaque utilisation s'engage à respecter les règles de déontologie informatique et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :

- De masquer sa véritable identité ;
- De se faire passer pour quelqu'un d'autre ;
- De s'approprier le mot de passe d'un autre utilisateur ;
- D'altérer des données ou d'accéder à des informations appartenant à d'autres utilisateurs du réseau, sans leur autorisation ;
- De porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants ;
- D'interrompre, sans y être autorisé, le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau ;
- De modifier ou de détruire des informations sur un des systèmes connectés au réseau ;
- De se connecter ou d'essayer de se connecter sur un site sans y être autorisé.
- La réalisation d'un programme informatique ayant de tels objectifs est également interdite.

SYSTÈMES INFORMATIQUES :

Les systèmes informatiques comprennent :

- L'ensemble des matériels à savoir : unité centrale ou station de travail (poste fixe ou portable) et tout autre matériel périphérique (écran, clavier, souris, imprimante/fax/copieur, scanner, appareil photo numérique, …), serveur réseau, câbles réseau, hub et routeur.
- L'ensemble des logiciels et progiciels contenus dans ou faisant fonctionner, communiquer ou protéger les ordinateurs et matériels informatiques.
- Ces logiciels comprennent également tous les protocoles de communication utilisés pour la mise en réseau des postes informatiques (TCP/IP, WINS, DNS, FTP) et permettant la constitution et la création, la duplication, la reproduction et le stockage des données, fichiers, bases de données, images, sons, textes, flux quelconques d'informations internes au réseau, avec l'extérieur, et quelle que soit la finalité de ces flux.

LE MAINTIEN EN BON ÉTAT D'UTILISATION DES MATÉRIELS :

Chaque utilisateur s'engage à prendre soin du matériel mis à sa disposition. Il informe le service informatique de toute anomalie constatée.

L'utilisateur s'engage à entretenir les périphériques dont il fait usage : écran, clavier, souris…
La nourriture et les boissons peuvent détériorer ces équipements.

BONNE UTILISATION DES LOGICIELS OU PROGICIELS :

Les postes de travail sont fournis avec les logiciels standards dont nous possédons les licences.
Certains logiciels optionnels ou spécifiques sont mis à disposition des utilisateurs ou d'une partie d'entre eux par le service informatique. Seul l'administrateur SSI peut installer ces logiciels. Il est alors demandé à tous de faire part de leurs besoins logiciels au service informatique.
Ces installations standards devraient suffire à combler les besoins professionnels des chacun.
En conséquence de quoi, il est interdit à tous :

- D'installer un autre logiciel sur son poste. Cela inclus les économiseurs d'écran, les jeux, les lecteurs de fichiers divers…. Cette liste n'étant pas exhaustive.
- De modifier la configuration du poste de travail sans y être autorisé au préalable par le service informatique.
- De réaliser une ou plusieurs copies d'un logiciel commercial ;
- De contourner les restrictions d'utilisation d'un logiciel ;
- De développer des programmes qui s'auto-dupliquent ou s'attachent à d'autres programmes (virus informatique).

A noter que le service informatique a le droit et la possibilité de verrouiller un logiciel.
Il est fortement recommandé aux agents de participer à des formations de mise à niveau.

PRESERVER LA SECURITE DU SYSTEME INFORMATIQUE.

Chaque utilisateur se voit attribuer un compte informatique et choisit un mot de passe qui lui permettra de se connecter au réseau. Ce mot de passe doit contenir au minimum 6 caractères et doit être modifié tous les 6 mois, faute de quoi, l'administrateur du réseau se verra le droit de forcer le changement.
Le compte informatique est strictement personnel et incessible. Chaque utilisateur est responsable de l'utilisation qui en est faite tout comme il est responsable de son mot de passe. Il s'engage à ne pas communiquer ce dernier à une tierce personne.
Il est demandé à tout utilisateur de verrouiller son poste informatique à chaque fois qu'il le quitte.

UTILISATION DES MOYENS INFORMATIQUES :

Disques et stockage :

Il est fortement conseillé d'enregistrer ses données sur le serveur et non sur le disque C dans la mesure où ce disque n'est jamais sauvegardé. De plus, le service informatique peut à tout moment être amené à réinstaller le poste de travail et dans ce cas, toutes les données présentes sur le disque sont effacées.
Les données qui sont présentes sur le serveur, elles, sont sauvegardées quotidiennement. Un fichier supprimé peut éventuellement être récupéré (consulter le service informatique).

Charte informatique DU SDIS DE LA MEUSE

La place disponible sur le serveur est limitée. Les grandes quantités de données allongent aussi les temps de sauvegarde. Aussi, est-il demandé à chacun de ne stocker que les données qui sont strictement nécessaires et de régulièrement trier les fichiers. Il est conseillé de pratiquer des archivages.
Chaque service dispose d'un espace dédié situé sur un serveur en réseau. Ce disque est destiné à accueillir les données communes à tout le service. En effet, tous les membres du service peuvent consulter et modifier les données qui s'y trouvent.
Concernant le stockage des données personnelles, un espace personnel nommé « USER » vous est alloué. Vous êtes le seul, excepté l'administrateur, à y avoir accès, sauf dérogation et organisation particulière.

Utilisation personnelle :

L'utilisation des outils à des fins personnelles est tolérée. Toutefois, une telle utilisation ne doit pas se faire de manière abusive, ni porter atteinte à l'intérêt et au bon fonctionnement du service.

MAITRISER LES TECHNOLOGIES INTERNET :

Utilisation d'Internet :

L'accès internet nécessite l'accord du chef de service et du directeur.
La navigation sur internet doit se limiter à la recherche et à la consultation d'informations à caractère professionnel.
Certains sites sont volontairement bloqués par le SSI :

- Sites à caractère pornographique ;
- Sites à contenu illégal ;
- Sites moralement répréhensibles : sites à caractère violent ou diffamatoire ou dont le contenu porte atteinte à la dignité humaine ;
- Sites de jeux en ligne ;
- Sites de certains médias ;
- Sites de réseaux sociaux….

L'accès à un site verrouillé peut être rétablit par le SSI s'il est nécessaire à l'activité de l'agent.
Il est interdit d'effectuer des téléchargements depuis internet et intranet, sauf autorisation exceptionnelle. Dans ce cas, la demande doit être formulée au SSI sous couvert du responsable hiérarchique.

Utilisation des systèmes de messagerie :

Chaque utilisateur se voit attribuer un compte de messagerie grâce auquel il peut dialoguer avec les autres agents du SDIS ainsi qu'avec d'autres personnes disposant d'une adresse de messagerie Internet (email).
Les comptes de messagerie sont paramétrés de façon identique pour tous les utilisateurs.
La messagerie est un outil de travail. L'échange de message non professionnels avec d'autres interlocuteurs dans et hors de l'établissement est cependant ponctuellement toléré. Aucune information d'ordre confidentiel, de fichier ludique et de chaîne de solidarité ne doivent être transférée.
Il est demandé aux utilisateurs de bien vouloir vider fréquemment leur boîte de messagerie et de faire des sauvegardes pour les messages les plus importants.
En dehors de demandes ou consignes particulières, des circonstances ou événements relatifs à la conduite ou au commandement des interventions, des missions confiées directement par lui, les agents sont tenus d'en référer à leur supérieur hiérarchique, pour la communication de messages au Directeur Départemental ou, en son absence, au Directeur adjoint.
Sauf mesures particulières, il est interdit de prendre connaissance et d'utiliser des informations détenues par d'autres utilisateurs quand bien même ceux-ci ne les auraient pas explicitement protégées.

REGLES D'UTILISATION DU TELEPHONE (Fixe et GSM) :

Comme pour internet et la messagerie électronique, sur le lieu de travail, l'utilisation du téléphone mis à disposition de l'agent doit présenter un caractère professionnel. Est simplement toléré un usage personnel du téléphone à condition de demeurer raisonnable, loyal et non préjudiciable au service.
Les numéros entrants et sortants à partir des postes sont enregistrés sur l'autocommutateur. Un logiciel spécifique permet d'accéder aux données stockées sur les autocommutateurs et d'analyser si besoin les trafics entrants et sortants sur chaque poste.

DECLARATION CNIL :

Ne pas divulguer d'informations confidentielles, notamment par téléphone, à des tiers qui ne doivent pas en avoir connaissance. Les traitements ou fichiers concernant des informations relatives à des personnes (nom, numéro…) doivent être déclarés à la CNIL, s'ils n'en sont pas expressément dispensés.
La loi informatique et libertés du 06 janvier 1978 modifiée fixe un ensemble de contraintes pour ces traitements : respect des finalités et des durées de conservation déclarées, information des personnes concernées, qui ont aussi un droit d'accès et de rectification aux donnés les concernant, accès sécurisé aux données et obligations de sauvegardes….

CONTROLE ET MAINTENANCE :

Seul le service informatique au titre de la sécurité dispose d'outils d'analyse, de surveillance et de contrôle. Le service informatique se réserve le droit de vérifier les contenus des répertoires et de supprimer les fichiers prohibés le cas échéant. La surveillance des connexions à internet, des flux d'information vers chaque messagerie est effectuée par ce dernier. Il dispose d'outils de prise en main à distance qui sont généralement employés pour dépanner les utilisateurs en leur montrant directement les manipulations qu'ils ont à faire.
Tenu au secret professionnel, le service informatique ne doit pas divulguer des informations qu'il aurait été amené à connaître dans le cadre de sa fonction et en particulier quand celle-ci est couverte par le secret des correspondances ou relève de la vie privée des utilisateurs et ne met en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni les intérêts de l'administration. Il ne saurait non plus être contraint de le faire, sauf disposition législative particulière.
En cas d'utilisation anormale du téléphone par l'utilisateur, à la demande expresse du directeur, il pourra être établi un relevé spécifique de l'ensemble des appels téléphoniques du poste de l'utilisateur faisant apparaître, pour chacun de ses appels, la date, la durée, le numéro du correspondant et le coût de la communication.
Pour tout ce qui concerne les demandes de dépannages et d'assistance, les agents doivent ouvrir un « ticket » via l'application GLPI SSI via intranet. Les demandes sont ensuite traitées par le service informatique.

SANCTIONS :

En cas de non-respect des règles et des principes exposés dans la charte d'utilisation, l'utilisateur s'expose, sans préjudices à d'éventuelles poursuites pénales, à des sanctions administratives.