DIRECTIVE

SUR

L'UTILISATION D'INTERNET, DES RESEAUX SOCIAUX, DE LA MESSAGERIE ELECTRONIQUE, DU TELEPHONE ET DU POSTE DE TRAVAIL

Table des matières **page**

1 But 2

2 Utilisation

2.1 Internet 2

2.2 Réseaux sociaux 2

2.3 Messagerie électronique 3

2.4 Téléphonie 3

2.5 Poste de travail et stockage des données 4

3 Contrôles

3.1 Contrôles globaux 4

3.2 Contrôles personnalisés 4

3.3 Instances compétentes 5

3.4 Mesures en cas d'abus 5

3.5 Conservation et traitement des données 5

1 BUT

1.1 Le but de la présente directive est de définir les droits et les devoirs des utilisateurs des moyens de communication (Internet, messagerie électronique, téléphonie) et des postes de travail informatiques mis à leur disposition dans le cadre professionnel, de prévenir une utilisation abusive de ces derniers et de régler les conséquences des éventuels abus.

2 UTILISATION

2.1 Internet

2.1.1 Internet doit être utilisé pour la recherche et la diffusion d'informations à but professionnel.

2.1.2 Une utilisation privée est admise à titre exceptionnel, en dehors des heures de travail, dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers), ne vise aucun but lucratif et ne viole pas le devoir de fidélité et de diligence de l'employé.

2.1.3 L'employeur peut bloquer l'accès à certaines catégories de sites Internet notamment :

- sites de messageries non professionnelles, y compris site de messagerie instantanée (« chat »);
- sites de transactions financières (notamment les sites boursiers) ou les sites payants;
- sites de jeux et de paris;
- sites à caractère érotique, violent ou raciste;
- sites qui sollicitent trop fortement les systèmes d'information (par ex. connexion à des sites radiophoniques).

2.1.4 Les collaborateurs ne consultent, ne stockent, ni ne diffusent des documents qui, sous quelque forme que ce soit, constituent une participation à un acte illicite et qui, en particulier, portent atteinte à la dignité de la personne, présentent un caractère pornographique, incitent à la haine raciale ou constituent une apologie du crime ou de la violence.

2.1.5 Les collaborateurs s'engagent à ne pas copier illégalement des logiciels, à ne pas diffuser des informations appartenant à des tiers sans leur autorisation et à mentionner les sources lors de l'utilisation d'informations en provenance de tiers.

2.1.6 Les collaborateurs ne sont pas autorisés à s'abonner à des services d'information payants, sauf autorisation de la Direction.

2.1.7 Les collaborateurs ne sont pas autorisés à télécharger des programmes, des jeux ou d'autres fichiers disponibles sur Internet, à réaliser des développements informatiques ou des modifications de la configuration des navigateurs Internet. Ces interventions sont effectuées par ou sous contrôle du Service informatique.

2.2 Réseaux sociaux

2.2.1 L'accès aux sites de réseaux sociaux, tels que Facebook, Twitter, LinkedIn, etc., n'est pas bloqué informatiquement.

2.2.2 L'utilisation de ces sites n'est possible durant les heures de travail que si elle a un but professionnel.

2.2.3 Il est interdit, même dans un but professionnel, de divulguer une quelconque information confidentielle par le biais de ces sites. Cela comprend également tout ce qui ressort du secret d'affaires, de la protection des marques et des droits d'auteurs.

2.2.4 Le collaborateur doit également respecter son devoir de diligence et de fidélité envers l'employeur lorsqu'il publie un texte dans le cadre d'une utilisation privée des réseaux sociaux. Il ne doit en aucun cas porter atteinte aux intérêts de son employeur.

2.3 Messagerie électronique

2.3.1 L'utilisation du courrier électronique comme instrument de communication est réservée aux besoins professionnels. Une utilisation privée est admise à titre exceptionnel, en dehors des heures de travail, dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers), ne vise aucun but lucratif et ne viole pas le devoir de fidélité et de diligence de l'employé. Pour des raisons de sécurité en cas d'utilisation privée, les collaborateurs ont recours à la messagerie professionnelle et non aux messageries personnelles privées (par ex. bluewin).

2.3.2 Les mentions suivantes doivent être utilisées dans les éléments d'adressage concernant la confidentialité ou le caractère privé/personnel d'un courrier électronique:

CONFIDENTIEL: Un courrier électronique dont les éléments d'adressage contiennent ce mot ne peut être ouvert que par les personnes ayant un accès explicite, en lecture, à la boîte aux lettres. Le traitement de l'information doit être traité de la même manière qu'un courrier confidentiel papier;

PRIVE ou PERSONNEL: Un courrier électronique dont les éléments d'adressage contiennent un de ces mots ne peut être ouvert que par la personne à qui le courrier électronique est destiné (dont le nom figure dans le texte ou fait partie de la désignation de la boîte aux lettres). Il ne doit contenir aucune information professionnelle.

Sans aucune précision, le courrier électronique peut être lu par des tierces personnes.

Le collaborateur est responsable d'informer les personnes susceptibles de lui faire parvenir des messages à caractère privé de la manière de rédiger le titre du message.

2.3.3 L'utilisation de fonctionnalités spéciales pour la messagerie (envoi automatique de notification de réception de messages, envois de SMS, etc.) est réservée exclusivement à des buts professionnels, dans la mesure où elle ne surcharge par l'infrastructure informatique. Les collaborateurs ne participent pas à des chaînes de distribution.

2.3.4 En cas de vacances, les collaborateurs prennent les mesures nécessaires pour assurer un suivi du courrier professionnel.

2.3.5 Les collaborateurs s'assurent de la source des fichiers attachés avant de les ouvrir. Les fichiers provenant d'une source inconnue doivent faire l'objet d'une attention particulière, notamment les extensions : .exe, .com, .bat, .xlm, .vbs, .vb. En cas de doute, les collaborateurs prennent contact avec le Service informatique.

2.3.6 Les collaborateurs ne consultent, ne stockent, ni ne diffusent des documents qui, sous quelque forme que ce soit, constituent une participation à un acte illicite et qui, en particulier, portent atteinte à la dignité de la personne, présentent un caractère pornographique, incitent à la haine raciale ou constituent une apologie du crime ou de la violence.

2.3.7 Chaque collaborateur s'engage à ne pas modifier les paramètres techniques, ni la liste de contrôles d'accès de sa messagerie personnelle.

2.3.8 Les collaborateurs s'engagent à ne pas diffuser des informations qui peuvent porter atteinte à la réputation de l'employeur.

2.4 Téléphonie

2.4.1 L'utilisation de la téléphonie fixe ou mobile est réservée aux besoins professionnels. L'utilisation de la téléphonie à usage privé est tolérée en respectant les points 2.4.2 à 2.4.4.

2.4.2 Pour les communications privées établies à partir d'un appareil de téléphonie fixe, les utilisateurs doivent composer, avant le numéro de l'appelé, le préfixe prévu à cet effet (10).

2.4.3 Dans tous les cas, les collaborateurs privilégient les appels depuis et vers les postes fixes avant de composer le numéro du mobile.

2.4.4 Les conversations privées doivent rester brèves et se limiter au plus petit nombre possible.

2.4.5 Les collaborateurs ont l'interdiction de communiquer à l'extérieur les numéros personnels directs autres que le leur.

2.4.6 L'utilisation de services payants et la commande de biens passée au moyen du téléphone et portée directement en compte sur la facture téléphonique sont interdites, sauf autorisation de la Direction.

2.5 Poste de travail et stockage des données

2.5.1 Le poste de travail est un élément constitutif du système informatique de l'employeur. La modification de son contenu et/ou un usage inapproprié peuvent avoir des effets sur le fonctionnement global du système. Le poste de travail doit être utilisé pour accomplir des tâches à buts professionnels.

2.5.2 Une utilisation privée des applications installées sur le poste de travail est tolérée à titre exceptionnel, en dehors des heures de travail, dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers), ne vise aucun but lucratif et ne viole pas le devoir de fidélité et de diligence de l'employé.

2.5.3 Sauf raison professionnelle justifiée et approuvée par la Direction, il est notamment interdit de:

- modifier la configuration matérielle du poste de travail en retirant des composants ou en installant des nouveaux (graveur, disque supplémentaire, lecteur DVD/CD-ROM, modem, etc.);
- connecter au poste de travail ou sur le réseau des appareils électroniques sans autorisation (agendas électroniques, téléphones portables, PC portables, clefs USB, etc.);
- modifier la configuration logicielle du poste de travail en retirant des programmes ou en installant des programmes téléchargés depuis Internet ou reçus par courrier électronique ou en provenance de toute autre source;
- réaliser des développements informatiques.

2.5.4 Les modifications effectuées, et qui sont interdites en vertu du chiffre 2.5.3 ci-dessus, seront supprimées sans préavis.

2.5.5 Les collaborateurs s'engagent à ne pas gêner les opérations découlant des besoins de gestion des postes de travail (activation d'outils d'inventaire et de diagnostic, de prise de main à distance, de télédistribution de logiciels, etc.).

2.5.6 Les collaborateurs s'engagent à traiter leur mot de passe personnellement et de manière confidentielle.

2.5.7 Les collaborateurs s'engagent à ne pas désactiver la protection antivirus.

2.5.8 De manière générale, les collaborateurs stockent leurs données sur les serveurs prévus à cet effet (cf. Directive sur l'organisation des dossiers informatiques). Ils sont tenus de les épurer régulièrement.

2.5.9 Les collaborateurs verrouillent leur poste de travail lorsqu'ils quittent leur place de travail. En cas d'absences prolongées (plus d'une heure) les collaborateurs ferment leur session. A la fin de leur journée de travail, ils éteignent leur poste de travail et leur écran.

3 CONTROLES

3.1 Contrôles globaux

3.1.1 Par contrôles globaux de l'utilisation d'Internet, on entend l'établissement de statistiques anonymes et aléatoires (effectuées de manière telle qu'elles ne permettent pas l'identification de l'utilisateur ou de l'utilisatrice) sur les sites les plus fréquemment visités, sur le nombre de connexions, sur le temps total passé à visiter des sites Internet ainsi que sur le volume du courrier électronique.

3.1.2 Le Responsable de la sécurité informatique effectue régulièrement des contrôles globaux, dans le respect des dispositions de la législation sur la protection des données. L'ouverture directe de fichiers ou de messages explicitement désignés comme données privées n'est pas autorisée, sauf accord du collaborateur.

3.1.3 Par contre, les utilisateurs sont informés que le personnel du service informatique (sous la supervision du Responsable de la sécurité informatique) peut avoir accès à n'importe quel moment à l'ensemble des composants du système, afin d'assurer sa protection et celle de ses collaborateurs et/ou de déceler des activités illégales.

3.1.4 Les résultats des contrôles globaux sont communiqués à la Direction.

3.2 Contrôles personnalisés

3.2.1 Lorsque les contrôles globaux, ou d'autres constatations, mettent en évidence des indices d'abus dans l'utilisation d'Internet, des contrôles personnalisés peuvent être effectués.

3.2.2 Par indices d'abus dans l'utilisation d'Internet, on entend, notamment pendant le temps de travail, un temps anormalement élevé d'utilisation par rapport aux tâches à effectuer, la visite fréquente de sites Internet paraissant ne pas avoir de lien avec la fonction ou, en tout temps, la visite de sites interdits.

3.2.3 En ce qui concerne le courrier électronique, le contrôle se limite en principe au nombre de messages envoyés et reçus, aux éléments d'adressage, aux types et volumes de fichiers attachés.

3.3 Instances compétentes

3.3.1 Les contrôles personnalisés sont ordonnés par la Direction.

3.3.2 La Direction nomme un Responsable de la sécurité informatique. Celui-ci effectue les contrôles.

3.3.3 Les informaticiens sont tenus au secret de fonction et ne peuvent divulguer, excepté au Responsable de la sécurité informatique, ni utiliser à leur avantage les informations dont ils auraient eu connaissance au cours d'actions de contrôle.

3.4 Mesures en cas d'abus

3.4.1 Après avoir entendu le collaborateur ou la collaboratrice et s'il s'avère que l'utilisation d'Internet et des moyens informatiques constitue une violation de la présente directive, la Direction prend les mesures appropriées, telles que le blocage de la boîte aux lettres ou de l'Internet et/ou des sanctions, qui peuvent aller de l'avertissement au licenciement immédiat pour justes motifs. Si les agissements du collaborateur sont de nature pénale, l'employeur peut porter plainte.

3.5 Conservation et traitement des données

3.5.1 Le Responsable de la sécurité informatique transmet l'ensemble des données récoltées dans le cadre des contrôles globaux et personnalisés à la Direction. Il ne conserve aucune de ces données.

3.5.2 La Direction peut conserver pendant six mois les données relatives aux contrôles personnalisés. Ces données sont ensuite détruites.

3.5.3 Est réservée la conservation de ces données au dossier d'une procédure disciplinaire.

3.5.4 Le traitement des données lors des contrôles personnalisés est confidentiel et soumis à la législation sur la protection des données.

Lieu, date