1 BUT

1.1 Le but de la présente directive est de définir les droits et les devoirs des utilisateurs à propos 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 d'éventuels abus. Cette directive fait partie intégrante du contrat de travail, et s'il y en a un du règlement d'entreprise. Elle s'applique à tous les collaborateurs et au personnel externe travaillant dans l'entreprise.

1.2 La direction nomme un responsable de la sécurité informatique. Ce dernier est chargé de l'application de cette directive et de son contrôle, conformément aux recommandations du préposé fédéral à la protection des données.

2 UTILISATION

2.1 Poste de travail et stockage des données

2.1.1 Le poste de travail est un élément constitutif du système informatique de l'entreprise. 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 professionnelles.

2.1.2 Sur le système central, et avec accord de l'employeur, un espace de stockage privé de taille raisonnable peut être créé, ceci afin de permettre au collaborateur de stocker des fichiers personnels. En aucun cas, l'entreprise ne pourra être tenue responsable de la sauvegarde et de la perte de ces données.

2.1.3 Une utilisation privée des applications installées sur le poste de travail est admise exceptionnellement, en dehors du temps 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) et ne viole pas le devoir de fidélité et de diligence de l'employé.

2.1.4 Sauf raison professionnelle justifiée, il est notamment interdit de :

- modifier la configuration matérielle du poste de travail en retirant des composants ou en installant de nouveaux (par exemple, 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;

Le GRI remercie les instances suivantes de leur fructueuse collaboration
Centre Patronal – Mme Catherine Staub – Secrétaire patronale – Tél 021/796 33 00
CVCI – Mme Norma Luzio – Sous-Directrice – Tél 021/613 35 35
FER de Genève – M. Bernard Collombara – Tél 022/715 33 33
Etude Delcò, Vollenweider, Blöchlinger – Me Denis Weber – Avocat - Tél 021/331 40 80
OPI – M. Valery Vouilloz – responsable marketing et TIC - Tél 022/717 84 00
Fondation Cognis – M. François Wollner – Vice-président – Tél 021/320 37 17

- réaliser des développements informatiques.

2.1.5 Les modifications effectuées en violation du chiffre 2.1.4 ci-dessus seront supprimées sans préavis.

2.1.6 Le collaborateur ne consulte, ni ne stocke ou ne diffuse des informations qui, sous quelque forme que ce soit, constituent notamment une participation à un acte illicite ou 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.

2.1.7 Le collaborateur s'engage à traiter son mot de passe personnellement et de manière confidentielle.

2.1.8 Le collaborateur s'engage à ne pas désactiver les protections.

2.1.9 De manière générale, le collaborateur stocke ses données sur les serveurs prévus à cet effet. Il est tenu de les épurer régulièrement.

2.1.10 Le collaborateur verrouille son poste de travail lorsqu'il quitte sa place de travail. En cas d'absence prolongée (plus d'une heure), le collaborateur quitte sa session. A la fin de la journée de travail, il éteint son poste de travail et son écran.

2.2 Internet

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

2.2.2 Une utilisation privée est admise en dehors du temps 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) ni ne viole le devoir de fidélité et de diligence de l'employé.

2.2.3 L'employeur se réserve le droit de bloquer, sans préavis, l'accès à certaines catégories de sites Internet, notamment :

- sites de messagerie non professionnelle, y compris site de messagerie instantanée (« chat »);
- sites de transactions financières (notamment les sites boursiers) ou ceux payants;
- sites de jeux et de paris;
- sites à caractère érotique, violent, raciste ou contraire aux mœurs de quelque manière que ce soit;
- sites qui sollicitent trop fortement les systèmes d'information (par ex. connexion à des sites radiophoniques).

2.2.4 Le collaborateur s'engage à ne pas copier illégalement des logiciels ou des fichiers protégés par un « copyright » (musique, film, *etc*.), à ne pas diffuser

Le GRI remercie les instances suivantes de leur fructueuse collaboration
Centre Patronal – Mme Catherine Staub – Secrétaire patronale – Tél 021/796 33 00
CVCI – Mme Norma Luzio – Sous-Directrice – Tél 021/613 35 35
FER de Genève – M. Bernard Collombara – Tél 022/715 33 33
Etude Delcò, Vollenweider, Blöchlinger – Me Denis Weber – Avocat - Tél 021/331 40 80
OPI – M. Valery Vouilloz – responsable marketing et TIC - Tél 022/717 84 00
Fondation Cognis – M. François Wollner – Vice-président – Tél 021/320 37 17

des informations appartenant à des tiers sans leur autorisation. Il s'engage à mentionner ses sources lors de l'utilisation d'informations.

2.2.5 Le collaborateur n'est pas autorisé à s'abonner à des services d'informations payants, sauf autorisation préalable.

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) et qu'elle ne viole pas le devoir de fidélité et de diligence de l'employé.

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 pourra 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. Le collaborateur s'engage notamment à ne pas contribuer à la propagation de chaînes de distribution.

2.3.4 En cas d'absence ou de vacances, le collaborateur prend les mesures nécessaires pour assurer un suivi de ses courriers électroniques professionnels.

2.3.5 Le collaborateur s'assure de la source des fichiers attachés avant de les ouvrir. Les fichiers provenant d'une source inconnue doivent faire l'objet

Le GRI remercie les instances suivantes de leur fructueuse collaboration
Centre Patronal – Mme Catherine Staub – Secrétaire patronale – Tél 021/796 33 00
CVCI – Mme Norma Luzio – Sous-Directrice – Tél 021/613 35 35
FER de Genève – M. Bernard Collombara – Tél 022/715 33 33
Etude Delcò, Vollenweider, Blöchlinger – Me Denis Weber – Avocat - Tél 021/331 40 80
OPI – M. Valery Vouilloz – responsable marketing et TIC - Tél 022/717 84 00
Fondation Cognis – M. François Wollner – Vice-président – Tél 021/320 37 17

d'une attention particulière notamment les extensions : .exe, .com, .bat, .xlm, .vbs, .vb. En cas de doute, il prend contact avec le Service informatique.

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

2.3.7 Le collaborateur s'engage à ne pas diffuser des informations qui peuvent porter atteinte à la réputation à l'entreprise.

2.3.8 Le collaborateur est rendu attentif au fait qu'un courrier électronique peut se transmettre très rapidement et qu'il doit donc être très prudent avec les informations qu'il véhicule, ceci spécialement pour des fichiers attachés à caractère confidentiel.

2.3.9 Si un collaborateur reçoit un courrier électronique à caractère violent, raciste ou pornographique, il est prié d'en avertir rapidement le responsable de la sécurité informatique. Ce dernier prendra les mesures nécessaires, afin de stopper ces réceptions non sollicitées.

2.3.10 Il est strictement interdit de transférer des courriers électroniques à caractère professionnel de son adresse professionnelle à son adresse privée.

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

2.4.2 L'utilisation de services payants, ainsi que la commande de biens portée directement en débit sur la facture téléphonique sont interdites, sauf autorisation de la Direction.

3 DEPART DU COLLABORATEUR

3.1.1 Au départ du collaborateur, et sans dispositions expresses contraires, son "adresse de courrier électronique" est immédiatement désactivée. Toute personne envoyant un courrier électronique à un collaborateur qui a quitté l'entreprise recevra un message clair, indiquant les nouvelles personnes de contact.

3.1.2 Le collaborateur s'engage à effacer, avant son départ, ses données personnelles de son "compte de courrier électronique" et de son espace privé.

4 CONTROLES ET MESURES DE SECURITE

4.1 Contrôles et mesures

4.1.1 L'employeur est attaché au respect de la vie privée des employés sur le lieu de travail et ce en respectant la législation sur la protection des données.

Le GRI remercie les instances suivantes de leur fructueuse collaboration
Centre Patronal – Mme Catherine Staub – Secrétaire patronale – Tél 021/796 33 00
CVCI – Mme Norma Luzio – Sous-Directrice – Tél 021/613 35 35
FER de Genève – M. Bernard Collombara – Tél 022/715 33 33
Etude Delcò, Vollenweider, Blöchlinger – Me Denis Weber – Avocat - Tél 021/331 40 80
OPI – M. Valery Vouilloz – responsable marketing et TIC - Tél 022/717 84 00
Fondation Cognis – M. François Wollner – Vice-président – Tél 021/320 37 17

4.1.2 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.

4.1.3 Le personnel du service informatique procédera à des contrôles anonymes et aléatoires des fichiers journalisés. Le traitement des données relevées est confidentiel et soumis à la protection des données.

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

4.2 Traitement des informations

4.2.1 En cas d'abus constaté, soit lorsque le présent règlement est violé, le responsable de la sécurité informatique procèdera à des analyses nominatives des fichiers.

4.3 Instances compétentes et sanctions en cas d'abus

4.3.1 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, par exemple, blocage de la boîte aux lettres ou de l'Internet, pénalité. Ces mesures peuvent aller jusqu'au licenciement, éventuellement pour justes motifs. Si les agissements du collaborateur sont de nature pénale, l'employeur se réserve tout droit.

Lu et approuvé par le collaborateur

Lieu et date : …… Signature du collaborateur

Le GRI remercie les instances suivantes de leur fructueuse collaboration
Centre Patronal – Mme Catherine Staub – Secrétaire patronale – Tél 021/796 33 00
CVCI – Mme Norma Luzio – Sous-Directrice – Tél 021/613 35 35
FER de Genève – M. Bernard Collombara – Tél 022/715 33 33
Etude Delcò, Vollenweider, Blöchlinger – Me Denis Weber – Avocat - Tél 021/331 40 80
OPI – M. Valery Vouilloz – responsable marketing et TIC - Tél 022/717 84 00
Fondation Cognis – M. François Wollner – Vice-président – Tél 021/320 37 17