Directive sur l'utilisation professionnelle des TIC

Station de travail - Internet
Messagerie électronique - Téléphonie

Version 2017

Domaine : Sécurité des systèmes d'information

Objectifs :
Le document présente une proposition de directive pouvant servir de base à chacun.
Il comprend :
- Le but de la directive
- Le champ d'application de la directive
- L'utilisation des moyens informatiques
  - Le poste de travail
  - Internet
  - La messagerie électronique
  - La téléphonie
- Les contrôles et mesures de sécurité
- Les règles à respecter lors du départ d'un collaborateur
- Les sanctions en cas d'abus

Public cible :

Toute personne susceptible de rédiger une directive d'entreprise concernant l'utilisation des outils informatiques comme : responsable informatique, responsable sécurité, responsable des ressources humaines, chef d'entreprise, etc.

Auteur : Groupement Romand de l'Informatique

Avertissement :
- Notre responsabilité nepeut être engagée, de quelque manière que ce soit, suite à l'utilisation du contenu de ce document.
- Cette publication utilise la forme masculine pour désigner les 2 genres et faciliter la lecture. Naturellement, toutes les formulations présentées concernent de manière égale les 2 genres.

GRI - Groupement Romand de l'Informatique
Rte de Genève 88
CH – 1004 Lausanne
Tél. : +41 (0)21 652 30 70
Fax : +41 (0)24 447 44 71
TVA : CHE 102.649.672
E-mail : gri@gri.ch
Internet : www.gri.ch

1 But

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

1.2 Cette directive fait partie intégrante du contrat de travail, et s'il y en a un du règlement d'entreprise.

2 Champ d'application

2.1 Cette directive s'applique à tous les collaborateurs de l'entreprise et au personnel externe travaillant pour l'entreprise ainsi qu'à tous les usagers occasionnels se connectant aux ressources de l'entreprise.

3 Infrastructure informatique

3.1 Principes directeurs

3.1.1 L'entreprise met à disposition de ses collaborateurs une infrastructure informatique afin de réaliser de manière efficace les tâches nécessaires à l'accomplissement de leurs fonctions et de permettre la communication couvrant les besoins professionnels.

3.2 Utilisation de l'infrastructure informatique

3.2.1 L'infrastructure informatique comprend l'ensemble des moyens matériels (stations de travail, serveurs, espaces de stockages, …), logiciels, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition de l'utilisateur.

3.2.2 L'informatique nomade tels que les assistants personnels, les ordinateurs portables, les téléphones portables … est également un des éléments constitutifs de l'infrastructure informatique.

3.2.3 La modification d'un des éléments de l'infrastructure informatique et/ou un usage inapproprié peuvent avoir des effets sur le fonctionnement global du système. Les composants mis à disposition doivent être utilisés pour accomplir des tâches professionnelles.

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

3.2.5 Une utilisation privée des applications mise à disposition 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 ou qu'elle ne soit pas contraire au code pénal.

3.2.6 L'usager s'engage, en outre, à ne pas stocker, diffuser ou accéder à 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, constituent une apologie du crime ou de la violence ou soient contraires au code pénal.

3.2.7 Sauf raison professionnelle justifiée et approuvée par l'employeur, il est notamment interdit de :

- modifier la configuration matérielle d'une station de travail en retirant des composants ou d'en installer

GRI - Groupement Romand de l'Informatique
Rte de Genève 88
CH – 1004 Lausanne
Tél. : +41 (0)21 652 30 70
Fax : +41 (0)24 447 44 71
TVA : 317875
E-mail : gri@gri.ch
Internet : www.gri.ch

de nouveaux (par exemple graveur, disque supplémentaire, lecteur DVD, modem, etc.);

- connecter à une station de travail ou au réseau des appareils électroniques sans autorisation (agendas électroniques, téléphones portables, PC portables, clefs USB, etc.);
- modifier la configuration logicielle d'une station de travail en retirant des programmes ou en installant des programmes téléchargés depuis Internet, reçus par courrier électronique ou en provenance de toute autre source;
- installer sans autorisation des environnements de stockage dans le nuage (cloud computing) tel que Dropbox ou autres à partir de l'environnement informatique de l'entreprise;
- réaliser des développements informatiques avec l'environnement informatique de l'entreprise.

Les modifications effectuées en violation de ce qui précède seront supprimées sans préavis. Leur auteur est passible de sanctions.

3.2.8 En cas d'autorisation, la connexion au réseau d'entreprise par un smartphone ou un PC portable privé n'est possible que par l'intermédiaire d'un réseau Wi-Fi prévu à cet effet. Si cela n'est pas possible, l'enregistrement d'appareil privé doit être demandé à l'employeur qui doit donner son autorisation pour le connecter au réseau fixe de l'entreprise.

3.2.9 Le collaborateur s'engage à traiter son mot de passe personnellement, de manière confidentielle et à l'actualiser selon les règles en vigueur dans l'entreprise.

3.2.10 Le collaborateur s'engage à ne jamais désactiver les protections mises en place.

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

3.2.12 Le collaborateur verrouille sa station 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 sa station de travail et son écran.

3.2.13 La gestion des stations de travail est effectuée par des personnes autorisées, sur le site ou à distance, en tout temps.

3.2.14 Le collaborateur s'engage à ne pas gêner les opérations découlant des besoins de gestion des stations de travail (activation d'outils d'inventaire et de diagnostic, de prise de main à distance, de télédistribution de logiciels, etc.).

3.2.15 Lorsque, dans le cadre d'une intervention, un collaborateur a connaissance de données à caractère confidentiel, il est tenu aux mêmes règles de confidentialité que l'utilisateur de la station de travail.

3.3 Internet

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

3.3.2 Une utilisation privé, y compris des réseaux sociaux, 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 ou qu'elle ne soit pas contraire au code pénal.

GRI - Groupement Romand de l'Informatique
Rte de Genève 88
CH – 1004 Lausanne
Tél. : +41 (0)21 652 30 70
Fax : +41 (0)24 447 44 71
TVA : 317875
E-mail : gri@gri.ch
Internet : www.gri.ch

3.3.3 L'employeur se réserve le droit de bloquer sans préavis l'accès à certaines catégories de sites Internet, et/ou de programmes, notamment :

- sites de messagerie non professionnelle, y compris sites de messagerie instantanée (chat, réseaux sociaux, ...);
- réseaux sociaux (autres que pour assurer la présence de l'entreprise sur la toile);
- sites de partage d'images ou de vidéos;
- sites de transactions financières (notamment les sites boursiers) ou ceux payants;
- sites de jeux ou de paris;
- sites à caractère érotique, violent, raciste ou contraire aux mœurs de quelque manière que ce soit; le cas échéant, tombant sous le coup de la loi;
- sites qui sollicitent trop fortement les ressources informatiques (par exemple connexion à des sites de diffusion audio ou vidéo);
- logiciels de vidéo conférence, téléphonie ou messagerie (Skype, ...).

3.3.4 Le collaborateur s'engage à ne pas copier illégalement des logiciels ou des fichiers protégés par un « copyright » (musique, films, œuvres littéraires, etc.), à ne pas diffuser des informations appartenant à des tiers sans leur autorisation. Il s'engage à mentionner ses sources lors de l'utilisation d'informations. L'utilisation de logiciels et/ou de sites de partage peer to peer (ou équivalent) est formellement interdite.

3.3.5 Le collaborateur s'engage à ne pas visualiser des émissions de télévision ou écouter des émissions radio pour lesquelles l'employeur n'a pas payé l'éventuelle redevance contractuelle.

3.3.6 Le collaborateur n'est pas autorisé, sauf autorisation préalable à :

- s'abonner à des services d'informations payants;
- utiliser un proxy (autre que celui éventuellement utilisé et installé par l'entreprise);
- utiliser un VPN donnant accès à un réseau externe (réseau privé virtuel);
- partager et/ou stocker des données sur un serveur externe à l'entreprise.

3.4 Messagerie électronique

3.4.1 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 ou qu'elle ne soit pas contraire au code pénal.

3.4.2 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;
- Privé ou Personnel : un courrier électronique dont les éléments d'adressage contiennent un de ces mots ne peut être ouvert que par la

GRI - Groupement Romand de l'Informatique
Rte de Genève 88
CH – 1004 Lausanne
Tél. : +41 (0)21 652 30 70
Fax : +41 (0)24 447 44 71
TVA : 317875
E-mail : gri@gri.ch
Internet : www.gri.ch

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.

3.4.3 L'utilisation de fonctionnalités spéciales de 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.

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

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

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

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

3.4.8 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.

3.4.9 A moins d'être cryptées, les données jugées sensibles relatives aux personnes ou à l'entreprise ne sont pas transmises par la messagerie électronique.

3.4.10 Si un collaborateur reçoit un courrier électronique à caractère violent, raciste, pornographique ou contraire au code pénal, 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.

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

3.5 Téléphonie

3.5.1 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.

3.5.2 L'utilisation de services payants, ainsi que la commande de biens (applications ou autres) portée directement en débit sur la facture téléphonique sont interdites, sauf autorisation de la Direction.

3.5.3 Le collaborateur a l'interdiction de communiquer à l'extérieur les numéros personnels directs autres que le sien.

3.5.4 Le débridage ou l'utilisation d'appareils débridés (jailbreak, appareils rootés, …) est strictement interdit dans le cadre d'une utilisation professionnelle.

3.5.5 Très gourmande en ressource réseau, la téléphonie par Internet ou VoIP (tel que Skype ou autre) est autorisée uniquement à des fins professionnelles et pour des besoins spécifiques. Les communications vidéo font l'objet des mêmes recommandations.

GRI - Groupement Romand de l'Informatique
Rte de Genève 88
CH – 1004 Lausanne
Tél. : +41 (0)21 652 30 70
Fax : +41 (0)24 447 44 71
TVA : 317875
E-mail : gri@gri.ch
Internet : www.gri.ch

3.6 L'enregistrement téléphonique

3.6.1 Principes directeurs

L'enregistrement des appels téléphoniques par l'employeur permet de :

- s'assurer de la qualité de l'accueil téléphonique;
- former les télésecrétaires, téléacteurs ou standardistes;
- fournir une preuve lors d'une réclamation;
- suivre le parcours des clients;
- améliorer le service.

L'enregistrement des appels téléphoniques de manière permanente permet de capturer l'intégralité des conversations téléphoniques, cette fonctionnalité apporte à l'entreprise des informations essentielles pouvant aider à :

- retracer un appel en cas de problème;
- se protéger lorsque la responsabilité de l'entreprise est engagée;
- maintenir le respect du règlement interne et externe;
- comprendre les besoins des clients.

L'enregistrement des appels téléphoniques que ce soit d'une manière ponctuelle ou permanente ne peut être réalisé que si :

- la nécessité est reconnue;
- l'enregistrement est proportionnel aux objectifs poursuivis.

3.6.2 L'enregistrement des appels téléphoniques par l'employeur est encadré par un dispositif légal qui vise à informer l'employé et ses interlocuteurs qu'ils peuvent faire l'objet d'un enregistrement de leurs conversations.

3.6.3 L'employé doit être informé par l'employeur que ses communications téléphoniques sont susceptibles d'être enregistrées en précisant :

- les objectifs de l'enregistrement téléphonique;
- les conséquences individuelles qui peuvent en découler;
- les salariés visés par le dispositif;
- les modalités de leur droit d'accès;
- les périodes des enregistrements téléphoniques.

3.6.4 Tous les partenaires qui appellent l'entreprise doivent être avertis que les communications téléphoniques peuvent faire l'objet d'un enregistrement téléphonique. Cette obligation consiste à :

- informer les clients de l'enregistrement dès le début de l'appel;
- donner les raisons de cet enregistrement.

La personne a le droit de refuser l'enregistrement. Dans ce cas l'entreprise se doit de lui proposer une alternative :

- ne pas enregistrer la conversation;
- se rendre directement dans les locaux de la société;
- utiliser les services Internet, ...

Au contraire, l'interlocuteur informé de l'enregistrement qui continue la communication donne son accord implicite pour que sa conversation soit enregistrée.

3.6.5 Ni information préalable au sujet de l'enregistrement de conversations téléphoniques, ni consentement de la personne concernée ne sont requis dans les cas suivants :

- lorsque la conversation implique des services d'assistance, de secours ou de sécurité (Art. 179quinquies al. 1 let. a), et

GRI - Groupement Romand de l'Informatique
Rte de Genève 88
CH – 1004 Lausanne
Tél. : +41 (0)21 652 30 70
Fax : +41 (0)24 447 44 71
TVA : 317875
E-mail : gri@gri.ch
Internet : www.gri.ch

- lorsque la conversation porte sur des commandes, des mandats, des réservations ou d'autres transactions commerciales de même nature, dans le cadre de relations d'affaires (Art. 179quinquies al. 1 let. b).

3.6.6 La durée de conservation des enregistrements téléphoniques doit être limitée et définie.

4 Départ du collaborateur

4.1.1 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.

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

5 Contrôle et mesures de sécurité

5.1 Principes directeurs

5.1.1 L'employeur nomme un Responsable de la sécurité informatique. Ce dernier est entre autre chargé de l'application de cette directive et de son contrôle, conformément aux recommandations du Préposé fédéral à la protection des données.

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

5.1.3 Pour assurer le respect de la présente directive, le Responsable de la sécurité effectue des contrôles anonymes et aléatoires, et, en cas de détection d'abus, des contrôles ciblés.

5.2 Contrôles anonymes et aléatoires

5.2.1 Les contrôles anonymes et aléatoires de l'utilisation des moyens de communication consistent au recueil et à l'analyse de statistiques sur la fréquence des visites sur différents sites, sur le nombre de connexions, sur le temps passé à chaque visite, sur le volume du courrier électronique, etc.

5.2.2 Les contrôles anonymes et aléatoires sont effectués en tout temps par le Responsable de la sécurité informatique dans le respect des dispositions de la législation sur la protection des données.

5.2.3 Le traitement des données relevées dans le cadre des contrôles anonymes et aléatoires est confidentiel et soumis à la protection des données.

5.2.4 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.

5.3 Contrôles ciblés

5.3.1 Des contrôles ciblés peuvent être entrepris lorsque les contrôles anonymes et aléatoires ou différentes constatations mettent en évidence des indices d'abus.

5.3.2 Les contrôles ciblés sont ordonnés par la Direction.

5.3.3 Les indices d'abus dans l'utilisation d'Internet comprennent notamment un temps anormalement élevé d'utilisation de ces moyens pendant le temps de travail par rapport aux tâches à effectuer, la visite fréquente de sites Internet paraissant ne pas avoir de lien avec la fonction, la visite de sites interdits.

5.3.4 Les contrôles d'abus dans l'utilisation des courriers électroniques se limitent

GRI - Groupement Romand de l'Informatique
Rte de Genève 88
CH – 1004 Lausanne
Tél. : +41 (0)21 652 30 70
Fax : +41 (0)24 447 44 71
TVA : 317875
E-mail : gri@gri.ch
Internet : www.gri.ch

en principe au nombre de messages envoyés et reçus, aux éléments d'adressage, aux types et volumes de fichiers attachés.

5.3.5 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.

5.4 Instances compétentes et sanctions en cas d'abus

5.4.1 Toute personne qui enfreint les dispositions de la présente directive s'expose à des mesures administratives ou disciplinaires en fonction de la gravité et des conséquences de son acte.

5.4.2 Après avoir entendu le collaborateur et si cela s'avère nécessaire, la Direction prendra les mesures appropriées (suppression des accès, remboursement des frais liés à l'utilisation abusive, mesures disciplinaires, poursuites judiciaires et/ou licenciement). Si les agissements du collaborateur sont de nature pénale, l'employeur se réserve tout droit.

6 For juridique

6.1.1 En cas de litige, le for juridique est celui de l'employeur.

Lu et approuvé par le collaborateur

Lieu et date : _____

Signature du collaborateur : _____

GRI - Groupement Romand de l'Informatique
Rte de Genève 88
CH – 1004 Lausanne
Tél. : +41 (0)21 652 30 70
Fax : +41 (0)24 447 44 71
TVA : 317875
E-mail : gri@gri.ch
Internet : www.gri.ch