

DIRECTIVE SUR L'UTILISATION DES OUTILS INFORMATIQUES A L'INTENTION DES UTILISATEURS DE L'ORIF

1. But

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) et des postes de travail informatiques mis à leur disposition dans le cadre professionnel, de prévenir une utilisation abusive, de garantir une utilisation optimale et de régler les conséquences d'éventuels abus. Cette directive fait partie intégrante du contrat de travail, du règlement d'entreprise et elle s'applique à tous les utilisateurs de l'Orif.

2. Utilisation

2.1. Poste de travail et stockage des données :

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.

Sur la station de travail, un espace de stockage privé, de taille raisonnable peut être créé, ceci afin de permettre à l'utilisateur de stocker des fichiers personnels. En aucun cas, l'entreprise ne pourra être tenue responsable de la sauvegarde, de la perte et de la confidentialité de ces données.

Une utilisation privée, à but non lucratif, 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 des utilisateurs.

Sauf autorisation du service IT, 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, etc.)
- connecter au poste de travail ou sur le réseau des appareils électroniques (agendas électroniques, téléphones portables, PC portables, clefs Wifi, disques durs, imprimante, scanner, etc.)
- modifier la configuration logicielle du poste de travail en retirant des programmes ou en installant des programmes (gratuits ou non) téléchargés depuis Internet, reçus par courrier électronique ou en provenance de toute autre source

Chaque utilisation interdite du matériel ou des logiciels sera signalée à la Direction du Centre.

Les modifications effectuées, en violation avec la liste ci-dessus, seront supprimées **sans préavis**.

L'utilisateur ne consulte sciemment, 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 érotique ou pornographique, incitent à la haine raciale ou constituent une apologie du crime ou de la violence.

L'utilisateur s'engage à traiter son mot de passe personnellement et de manière confidentielle. Ce dernier est responsable de son utilisation abusive.

L'utilisateur s'engage à ne pas désactiver les protections.

De manière générale, l'utilisateur stocke ses données sur les serveurs prévus à cet effet. Il est tenu de les épurer régulièrement. Une limite de stockage est fixée par le service IT.

L'utilisateur verrouille son poste de travail lorsqu'il quitte sa place. En cas d'absence prolongée et durant la pause de midi, l'utilisateur quitte sa session. A la fin de la journée de travail, sauf avis contraire du service IT, il éteint son poste de travail et son écran.

2.2. Internet :

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

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.

Le service IT et / ou la Direction du Centre se réservent 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 (MSN, Yahoo, chat en tout genre ...).
- Sites de réseaux sociaux (facebook, twitter, ...), sauf accord préalable du Service IT.
- sites de transactions financières (notamment les sites boursiers) d'achat en ligne ou ceux payants.
- sites de jeux et de paris.
- sites à caractère érotique et pornographique.
- sites violent, racistes ou contraire aux mœurs de quelque manière que ce soit.
- sites qui sollicitent trop fortement les systèmes d'information (par exemple : sites radiophoniques ou télévisuels).

L'utilisateur s'engage à ne pas copier illégalement des logiciels ou des fichiers protégés par un « copyright » (images, musique, film, 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'utilisateur n'est pas autorisé à s'abonner à des services d'informations payants, sauf autorisation préalable du service IT.

2.3. Messagerie électronique (si applicable) :

L'utilisation du courrier électronique, mis à disposition par l'Orif 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.

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. La gestion de l'information doit être traitée 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 l'objet du message 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.

L'utilisateur est responsable d'informer les personnes susceptibles de lui faire parvenir des messages à caractère privé, de la manière d'en rédiger le titre.

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 pas l'infrastructure informatique. L'utilisateur s'engage notamment à ne pas contribuer à la propagation de chaînes de distribution.

En cas d'absence ou de vacances, l'utilisateur prend les mesures nécessaires pour assurer un suivi de ses courriers électroniques professionnels et/ou avertir l'expéditeur.

L'utilisateur 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, zip, rar, ...

En cas de doute, il prend contact avec le Service IT.

Chaque utilisateur s'engage à ne pas modifier les paramètres techniques, ni ceux de sa messagerie.

L'utilisateur s'engage à ne pas diffuser des informations qui peuvent porter atteinte à la réputation de l'entreprise.

L'utilisateur 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. Il est également rendu attentif que les courriers électroniques sont transmis en clair sur Internet, ils peuvent donc être interceptés et lus par des personnes mal intentionnées.

Si un utilisateur reçoit un courrier électronique à caractère violent, raciste ou pornographique ou contraire aux bonnes mœurs, il est prié d'en avertir rapidement le responsable informatique local. Ce dernier prendra les mesures nécessaires, afin de stopper ces réceptions non sollicitées.

Il est interdit de transférer des courriers électroniques à caractère professionnel, de son adresse professionnelle à son adresse privée, sauf dérogation du Directeur du Centre.

3. Départ de l'utilisateur

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

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

4. Contrôles et mesures de sécurité

4.1. Contrôles et mesures

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

Par contre, les utilisateurs sont informés que le personnel du Service 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 utilisateurs et/ou de déceler des activités illégales.

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.

Les collaborateurs du Service IT sont tenus au secret de fonction et ne peuvent divulguer, ou utiliser à leur avantage, les informations dont ils auraient eu connaissance au cours d'actions de contrôle.

4.2. Traitement des informations :

En cas d'abus constaté, soit lorsque le présent règlement est violé, la CPPI (Commission de Planification et Pilotage Informatique) nommera un responsable qui procédera à des analyses nominatives des fichiers. Il établira un rapport qui sera transmis au Directeur général.

4.3. Instances compétentes et sanctions en cas d'abus :

Après avoir entendu l'utilisateur, et s'il s'avère que l'utilisation d'Internet et des moyens informatiques constitue une violation de la présente directive, les Directions locales et la Direction Générale prendront les mesures appropriées. L'utilisateur peut faire l'objet d'une suspension ou d'un renvoi définitif. Si les agissements de l'utilisateur sont de nature pénale, l'Orif se réserve tout droit.

4.4. Engagement personnel de respect :

Les assurés placés à l'Orif reçoivent à leur admission la présente directive en vigueur. En signant la feuille de compte utilisateur reçue via son MSP, ils s'engagent à la respecter.

Les collaborateurs et les autres utilisateurs reçoivent la présente directive en vigueur. En signant la feuille de compte utilisateur reçue via le Service IT, ils s'engagent à la respecter.