Annexe 1 au Règlement intérieur

Charte de Sécurité Informatique d'ALLO-MEDIA

Introduction

Allo-Media met en œuvre un système d'information et de communication nécessaire à l'exercice de son activité. Allo-Media met ainsi à disposition de ses collaborateurs des outils informatiques, et de communication.

La présente charte a pour objet de réglementer et de contrôler l'usage des nouvelles technologies de l'information et de la communication. Elle définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication d'Allo-Media.

Elle a également pour objet desensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et / ou pénale ainsi que celle de Allo-Media.

Responsable de la Sécurité Informatique

Allo-Media a désigné Rémy LAPLEIGE comme responsable de la sécurité informatique. Il est obligatoirement consulté pour toutes demandes de traitement informatique.

LE CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à tout utilisateur du Système d'Information et de communication de l'entreprise, pour l'exercice de ses activités professionnelles. L'utilisation à titre privé de ces outils est tolérée, mais doit être raisonnable et ne pas perturber le bon fonctionnement du service.

La charte est diffusée à l'ensemble des utilisateurs par note de service et, à ce titre, mise à disposition sur le système d'intranet d'Allo-Média. Elle est systématiquement remise à tout nouvel arrivant.

Des actions de communication internes sont organisées régulièrement afin d'informer les utilisateurs des pratiques recommandées.

Quelques définitions :

On désignera sous le terme « **utilisateur »** toute personne autorisée à accéder aux outils informatiques et aux moyens de communication d'Allo-Média et à les utiliser : employés, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels….

Les termes « **outils informatiques et de communication** » recouvrent tous les équipements informatiques, de télécommunications et de reprographie d'Allo-Media.

I - LES REGLES D'UTILISATION DU SYSTEME D'INFORMATION D'ALLO-MEDIA

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies par Allo-Media.

1 - Les modalités d'intervention du service de l'informatique interne

Le service de l'informatique interne assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication au sein de l'entreprise.

Les collaborateurs du service informatique de l'entreprise disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Ils ont accès à l'ensemble des données techniques mais s'engagent à respecter les règles de confidentialité applicables aux contenus des documents.

Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

1.1 - L'authentification

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte (« login » ou identifiant) fourni à l'utilisateur lors de son arrivée à/chez Allo-Media. Un mot de passe est associé à cet identifiant de connexion

Les moyens d'authentification sont personnels et confidentiels.

Actuellement, le mot de passe doit être composé de 12 caractères minimum combinant chiffres, minuscules, majuscules et caractères spéciaux. Il ne doit comporter ni le nom, prénom ni l'identifiant d'ouverture de la session de travail. Il doit être renouvelé tous les trois mois.

1.2 - Les règles de sécurité

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler au service informatique interne d'Allo-Media toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.
- Ne jamais confier son identifiant/mot de passe.
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur.

- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identitéd'autrui.
- Ne pas modifier les paramétrages du poste de travail.
- Ne pas installer de logiciels sansautorisation.
- Ne pas copier, modifier, détruire les logiciels propriétés d'Allo-Media.
- Verrouiller son ordinateur dès qu'il quitte son poste de travail.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- Toute copie de données sur un support externe est soumise à l'accord du supérieur hiérarchique et doit respecter les règles définies par Allo-Media.

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au Système d'Information d'Allo-Media sans l'accord préalable du service informatique interne.

Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre Allo-Media et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

II - LES MOYENS INFORMATIQUES

1 - Configuration du poste de travail

Allo-Média met à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions. L''utilisateur ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle sans y avoir explicitement été autorisé par l'équipe informatique interne.
- Connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par l'équipe informatique interne.
- Déplacer l'équipement informatique (sauf s'il s'agit d'un « équipement nomade »)
- Nuire au fonctionnement des outils informatiques et de communications.

Toute installation de logiciels supplémentaires (exemple : logiciels de consultation de fichiers multimedia) est subordonnée à l'accord du service informatique interne.

1.1 - Sécuriser l'accès au compte

Le contrôle d'accès logique permet d'authentifier l'accès de toute personne utilisant un ordinateur.

Cette authentification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.

Une authentification (login + mot de passe) unique est confiée à chaque utilisateur. Ce dernier est personnellement responsable de l'utilisation qui peut en être faite, et ne doit en aucun cas la communiquer.

2- Equipements nomades et procédures spécifiques aux matériels de prêt

2.1 - Equipements nomades

On entend par « **équipements nomades** » tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD ROM, clé USB etc...).

Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.

L'utilisation de smartphones pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

2.2 - Procédures spécifiques aux matériels de prêt

L'utilisateur doit renseigner et signer un registre, tenu par le service informatique interne, actant la remise de l'équipement nomade ou encore la mise à disposition d'un matériel spécifique pour la tenue d'une réunion (vidéo-projecteur). Il en assure la garde et la responsabilité et doit informer la direction générale en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte. Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements. Le retour du matériel est consigné dans le registre.

3 - Internet

3.1 – Sites internet consultables

Les utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient.

Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, l'ordre public, et ne met pas en cause l'intérêt et la réputation de l'institution, est admise.

Chaque utilisateur doit prendre conscience qu'il est dangereux pour l'entreprise :

- de communiquer à des tiers des informations techniques concernant son matériel ;
- de diffuser des informations sur l'entreprise via des sites Internet ;
- de participer à des forums (même professionnels) ;
- de participer à des conversations en ligne (« chat »).

3.2 - Pare-feu

Le pare-feu vérifie tout le trafic sortant de l'entreprise, aussi bien local que distant. Il vérifie également le trafic entrant constitué de la messagerie électronique, l'échange de fichiers, et la navigation sur Internet.

Il détient toutes les traces de l'activité qui transite par lui s'agissant :

- de la navigation sur Internet : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels) ;
- des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe *(et éventuellement texte du message)*.

Il filtre les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste ou contenant des données jugées comme offensantes.

4 - Courrier électronique

4.1 Conditions d'utilisation

La messagerie mise à disposition des utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée, à la condition de ne pas affecter le trafic normal des messages professionnels et si elle n'affecte pas le travail du collaborateur ni la sécurité du réseau informatique de l'entreprise.

Tout message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

Allo-Média s'interdit d'accéder aux dossiers et aux messages identifiés comme « personnel » dans l'objet de la messagerie du collaborateur sans avoir obtenu son consentement préalable.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par le service informatique interne, et validées par la direction technique :

- volumétrie de la messagerie,
- taille maximale de l'envoi et de la réception d'un message,
- nombre limité de destinataires simultanés lors de l'envoi d'un message,
- gestion de l'archivage de lamessagerie.

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur supports externes.

Les collaborateurs peuvent consulter leur messagerie à distance, à l'aide d'un navigateur (webmail). Les fichiers qui seraient copiés sur l'ordinateur utilisé par le collaborateur dans ce cadre doivent être effacés dès que possible de l'ordinateur utilisé.

4.2 - Consultation de la messagerie

En cas d'absence d'un collaborateur et afin de ne pas interrompre le fonctionnement du service, le service informatique peut, ponctuellement transmettre au supérieur hiérarchique un message électronique à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur.

Le supérieur hiérarchique n'a pas accès aux autres messages du collaborateur. Le collaborateur concerné est informé dès que possible de la liste des messages qui ont été transférés.

En cas d'absence prolongée d'un collaborateur (longue maladie), le chef de service peut demander au service informatique, après accord de son directeur, le transfert des messages reçus.

4.3 - Courriel non sollicité

Allo-Média dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

4.4 - Utilisation privée de la messagerie

L'utilisation du courrier électronique à des fins personnelles est autorisée dans des proportions raisonnables et à la condition de ne pas affecter le trafic normal des messages professionnels.

À ce titre, les salariés devront identifier leurs messages et fichiers personnels de façon à ne pas les confondre avec les messages reçus à titre professionnel : qualification par l'objet, création d'un répertoire spécifique dédié au contenu privé.

4.5 - Contrôle de l'usage

Dans l'hypothèse la plus courante, le contrôle éventuellement mis en œuvre porte sur :

- le nombre des messages échangés par utilisateur ;
- la taille des messages échangés ;
- le format des pièces jointes.

4.6 – Droit à la déconnexion et à la régulation de l'utilisation des outils numériques

Cette charte a pour but de définir les modalités du plein exercice par le salarié de son droit à la déconnexion et la mise en place par l'entreprise de dispositifs de régulation de l'utilisation des outils numériques en vue d'assurer le respect des temps de repos et de congés ainsi que la vie personnelle et familiale.

À cette fin, les mesures qui ont été prises, sont les suivantes:

- les salariés ne sont pas tenus de se connecter à leur adresse e-mail professionnelle en dehors des heures de travail ou des plages de travail pour les salariés sous forfait jours, le week-end, les jours fériés, pendant les congés payés, les arrêts maladie, les congés maternité, etc. ;
- l'utilisation du téléphone portable et/ou de l'ordinateur professionnel est limitée aux heures de travail *ou* des plages de travail pour les salariés sous forfait jours) ;
- tous les appareils connectés doivent être éteints en dehors des heures de travail ou des plages de travail pour les salariés sous forfait jours ;
- aucun e-mail ou SMS professionnel ne doit être envoyé, lu ou traité en dehors des heures de travail ou des plages de travail pour les salariés sous forfait jours ;
- une mention est intégrée dans chaque signature électronique afin d'informer les interlocuteurs de l'absence d'obligation de traiter les e-mails en dehors des heures de travail ou des plages de travail pour les salariés sous forfait jours ;
- etc.

Ce droit à la déconnexion concerne tous les salariés, cadres et non-cadres, y compris les salariés en télétravail.

Les managers sont informés de cette charte et veilleront à son respect, notamment par des actions de sensibilisation et/ou contraignantes telles que le contrôle des connexions à distance.

D'autre part, sauf en cas d'urgence, les managers veilleront à ne pas solliciter les salariés en dehors des heures de travail ou des plages de travail pour les salariés sous forfait jours.

5 - Téléphone

Allo-Média met à disposition de certains utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles.

L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable.

Des restrictions d'utilisation par les collaborateurs des téléphones fixes sont mises en place en tenant compte de leurs missions. A titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

Allo-Média s'interdit de mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Elle vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

III - L'ADMINISTRATION DU SYSTEME D'INFORMATION

Afin de surveiller le fonctionnement et de garantir la sécurité du système d'information, différents dispositifs sont mis en place.

1 – Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information pour Allo-Média et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles (peer to peer, messagerie instantanée…).

2 – Les systèmes automatiques de traçabilité

Le service informatique d'Allo-Média opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité.

Il s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données suivantes : dates, postes de travail et objet de l'évènement.
Le service informatique est le seul utilisateur de ces informations qui sont effacées à l'expiration d'un délai de trois mois.

3 - Gestion du poste de travail

A des fins de maintenance informatique, le service informatique interne d'Allo-Média peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur.

Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, le service informatique peut être amené à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus.

4 - Sauvegardes

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde des informations sur les répertoires partagés.

Ceci implique, entre autres, que la suppression par un utilisateur d'un fichier des répertoires partagés n'est pas absolue et qu'il en reste une copie :

- sur le dispositif de sauvegarde;
- sur le serveur ;
- sur le proxy.

IV PROCEDURE APPLICABLE LORS DU DEPART DE L'UTILISATEUR

Lors de son départ, l'utilisateur doit restituer au service de l'informatique interne les matériels mis à sa disposition.

Il doit préalablement effacer ses fichiers et données privées au plus tard le jour de son départ effectif de l'entreprise. Toute copie de documents professionnels est formellement interdite sauf autorisation écrite du responsable de service.

Les comptes et les données personnelles de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ.

V - RESPONSABILITES- SANCTIONS

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre.

Des sanctions en interne peuvent être prononcées, elles consistent :

- dans un premier temps, en un rappel à l'ordre en cas de non-respect des règles énoncées par la charte ;
- dans un second temps, et en cas de renouvellement,] en des sanctions disciplinaires adaptées.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information (cf. liste des textes en annexe) est susceptible de sanctions pénales prévues par la loi.

ENTREE EN VIGUEUR DE LA CHARTE

La présente charte est applicable à compter du 28 décembre 2017.

Fait à Paris, le 16 février 2017

Monsieur Romain SAMBARINO
Président

Dépôt au Conseil des prud'hommes comme annexe au Règlement intérieur