ACCEPTATION D'INTERNET ET DES OUTILS DE COMMUNICATION ÉLECTRONIQUE UTILISATION POSSIBLE POLITIQUE RELATIVE AUX PROCÉDURES ET AUX PRINCIPES

KVKK_P9 VERSION 1.00

KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED COMPANY

INTERNET ET OUTILS DE COMMUNICATION ÉLECTRONIQUE PROCÉDURES RELATIVES À L'UTILISATION ACCEPTABLE

POLITIQUE RELATIVE AUX PRINCIPES

1. INTRODUCTION

La société Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi, en tant qu'entité juridique privée, est tenue de veiller à la bonne utilisation de toutes les ressources de l'entreprise qui lui sont allouées et d'empêcher tout usage abusif ou inapproprié non conforme à leur finalité. Cette responsabilité inclut l'utilisation de services tels que la messagerie électronique et l'accès à Internet.

2. OBJET ET PORTÉE

La présente politique a pour objet de définir les procédures et les principes que les employés de notre entreprise doivent respecter lorsqu'ils utilisent des moyens de communication électroniques tels qu'Internet et le courrier électronique. Elle se compose de trois parties :

- Politique d'utilisation d'Internet • Politique d'utilisation du courrier électronique
- Communications électroniques entre employés

La présente politique doit être considérée conjointement avec les documents de politique suivants :

- Règlement disciplinaire de l'entreprise
- Politique de protection et de traitement des données
- Politique de sécurité de l'information

Aux fins de la présente politique, toute forme de communication électronique, y compris le courrier électronique, la messagerie Web, la messagerie instantanée et les forums Web, est considérée comme une forme de communication électronique. Si l'accès à Internet et à la messagerie électronique fourni par la Société est utilisé via un réseau sans fil au sein des locaux de la Société ou via un ordinateur depuis l'extérieur, la personne concernée sera réputée avoir accepté les dispositions de la présente instruction.

3. POLITIQUE D'UTILISATION D'INTERNET

3.1. Objectifs de la prestation de services et responsabilités des utilisateurs :

L'accès à Internet est initialement et principalement destiné aux activités de l'entreprise. Son utilisation à titre personnel est acceptable, à condition qu'elle soit raisonnable, respectueuse et responsable, notamment lorsque les employés y accèdent pour des raisons personnelles.

3.2. Suivi de l'utilisation :

3.2.1. Les employés utilisant le réseau internet de l'entreprise ne peuvent raisonnablement s'attendre à aucune confidentialité ni à aucune protection de leur vie privée. L'entreprise utilise des sites et des liens sécurisés pour enregistrer les recherches internet et empêcher tout accès inapproprié.

Le système utilise les services suivants . Il est géré par le responsable informatique et supervisé par les chefs de service et le conseil d'administration. Le pare-feu est testé périodiquement afin de détecter toute défaillance ou faille potentielle du système.

3.2.2. Logiciel de surveillance. Ce logiciel surveille l'utilisation du réseau Internet de l'entreprise. Le service informatique et les responsables de service consultent et auditent les journaux de connexion afin de garantir une utilisation conforme aux politiques de l'entreprise. Cela inclut l'analyse à distance des écrans d'ordinateur, la vérification des fichiers et des courriels, ainsi que l'analyse des sites web consultés. Le logiciel enregistre tous les sites web visités, ainsi que le nom d'utilisateur et les détails de la date et de l'heure de visite, et génère des rapports réguliers à des fins de surveillance. Les visites et les sites web abusifs ou suspects sont automatiquement signalés et les procédures disciplinaires standard sont mises en œuvre. En accédant au réseau Internet de l'entreprise, les utilisateurs sont réputés avoir consenti aux activités de surveillance et de contrôle d'accès Internet décrites ci-dessus.

3.3. Abonnement personnel et utilisation de loisirs :

Les employés ne sont pas autorisés à souscrire à des abonnements auprès de fournisseurs d'accès Internet ou à des services en ligne au sein de l'entreprise et à les utiliser sur le matériel informatique de celle-ci sans l'accord écrit du responsable informatique. L'utilisation d'Internet à des fins de divertissement inappropriées, telles que les jeux vidéo ou les jeux d'argent, est interdite.

3.4. Actions susceptibles de nuire à la réputation de l'entreprise :

Les employés ne sont pas autorisés à utiliser Internet d'une manière contraire aux intérêts de l'entreprise, susceptible de lui porter préjudice, ainsi qu'à ses partenaires, ou de nuire à sa réputation. Par exemple, s'abonner à des sites web proposant des contenus interdits ou illégaux, ou utiliser ou télécharger des contenus protégés par le droit d'auteur auprès de tiers sans l'autorisation expresse du titulaire des droits.

3.5. Installation du logiciel (téléchargement) :

Afin de minimiser les risques de virus et d'empêcher la présence de logiciels non autorisés sur le réseau, l'installation de logiciels via le réseau de l'entreprise est interdite. Cette interdiction s'applique également aux jeux et aux économiseurs d'écran. Si une exception à cette interdiction est nécessaire à des fins de formation du personnel, veuillez contacter le service informatique.

3.6. Utilisation illégale :

Il est interdit aux employés d'utiliser sciemment Internet pour des activités enfreignant la législation turque. Ils ne sont pas autorisés à utiliser Internet pour rechercher, télécharger, consulter ou consulter des contenus susceptibles d'offenser ou de discriminer d'autres employés en raison de leur sexe, de leur origine ethnique, de leurs convictions religieuses, de leur orientation sexuelle, de leur handicap ou pour tout autre motif.

3.7. Achats en ligne :

Les employés peuvent être autorisés à effectuer des achats en ligne pendant leurs heures de travail prolongées. Toutefois, il est important de rappeler qu'il est interdit d'installer le logiciel du vendeur sur votre ordinateur ou tout autre appareil. Bien que le réseau fourni n'offre pas des normes de sécurité inférieures à celles des réseaux résidentiels, notre société ne peut être tenue responsable de la sécurité des transactions financières. Les achats ne doivent en aucun cas inclure des articles obscènes, pornographiques ou portant atteinte à la vie privée, ni aucune activité interdite.

3.8. Sécurité :

En tant qu'employés responsables de l'accès au réseau et de sa sécurité, il est essentiel que vous ne partagiez jamais votre nom d'utilisateur et votre mot de passe. À cet égard, vous devez verrouiller votre ordinateur lorsque vous vous en éloignez en appuyant sur Ctrl+Alt+L ou Ctrl+Alt+Suppr. En cas de perte ou de vol d'un appareil personnel utilisé pour accéder à la messagerie ou aux données de l'entreprise, le service informatique doit en être immédiatement informé. Nos employés doivent également prendre connaissance de la politique de sécurité des systèmes d'information, qui contient des informations détaillées sur la protection des mots de passe et la sécurité.

3.9. Activités interdites :

Les activités interdites sur Internet comprennent les outils suivants :
Cela inclut la surveillance, le stockage, la distribution ou toute autre utilisation du produit.

• Activités illégales (y compris toutes les formes de violation du droit d'auteur) •
Comportements menaçants, abusifs, harcelants ou discriminatoires
• Toute
forme de diffamation, intention et activité
calomnieuse • Tout message obscène, provocateur ou à caractère privé, toute image choquante
ou tout contenu pornographique • Tout
élément susceptible de nuire à notre société sans autorisation préalable
activités

• Chaînes de lettres envoyées par courriel • Activités individuelles ou commerciales menées à but lucratif • Actes malveillants et nuisibles • Utilisations inappropriées à des fins politiques, religieuses ou de divertissement.

3.10. Obligation de protéger :

Tout employé qui entre accidentellement en contact avec des images à caractère pédopornographique lors de l'utilisation du réseau de l'entreprise doit immédiatement signaler l'emplacement de ces images au service informatique et ne doit ni en faire de copies ni les diffuser à qui que ce soit

3.11. Considérations relatives à la sécurité et à l'accès :

3.11.1. L'entreprise a mis en œuvre des mesures de sécurité pour protéger ses systèmes informatiques, ses sites web et ses employés contre les menaces de sécurité externes et internes, actuelles et potentielles. Ces mesures comprennent notamment : des pare-feu et des serveurs proxy pour bloquer le trafic internet entrant et sortant ; des logiciels antivirus ; des logiciels de contrôle d'accès (bloquant l'accès à certains sites web) ; des mesures de prévention de l'installation de logiciels ; et des logiciels bloquant les scripts et éléments potentiellement dangereux.

3.11.2. La Société bénéficie de services de filtrage fournis par son serveur Internet. Bien que l'accès à Internet ne soit pas bloqué pour ses employés utilisant son réseau, la Société peut bloquer l'accès aux sites contenant, ou susceptibles de contenir, des contenus illégaux, pornographiques ou choquants (par exemple, messages à caractère sexuel explicite, messagerie instantanée, activités criminelles, drogues, alcool et tabac, jeux d'argent, sites de rencontre, forums Usenet, violence et armes, etc.).

3.11.3. Les utilisateurs d'Internet doivent savoir que de nombreux sites Web enregistrent parfois secrètement des détails sur l'utilisation du site et que l'accès et l'activité sur Internet laissent un journal sur leur PC.

3.11.4. La Société se réserve le droit d'interrompre l'accès à Internet sans préavis si elle soupçonne une faille de sécurité nécessitant une action immédiate ou si elle estime que le réseau et/ou les systèmes informatiques de la Société sont menacés.

4. POLITIQUE ET DIRECTIVES RELATIVES AUX COURRIELS

4.1. La présente politique a pour but d'assurer la bonne utilisation des systèmes de messagerie électronique.
Tout employé autorisé à accéder au service de messagerie est tenu de respecter les dispositions de la présente politique et de veiller à ce que le système de messagerie soit utilisé de manière responsable, efficace et uniquement à des fins approuvées. Cette politique a pour but de fournir des informations servant de guide aux employés, notamment en ce qui concerne les communications internes de l'entreprise par courriel. Par exemple, l'utilisation personnelle du système de messagerie de l'entreprise est interdite.

4.2. État des communications par courriel :

Nos employés doivent toujours garder à l'esprit que les échanges par courriel constituent des documents pouvant être utilisés comme preuves dans le cadre de procédures judiciaires. Tous les courriels envoyés ou reçus sur le réseau de messagerie de notre entreprise sont la propriété de celle-ci, et les utilisateurs ne doivent pas s'attendre à une confidentialité absolue de leurs communications. Le service informatique est habilité à surveiller les courriels et les journaux réseau afin de garantir le respect des politiques de l'entreprise. Tout utilisateur est réputé avoir consenti à cette surveillance et à cet examen de ses courriels.

4.3. Courriels personnels :

Les utilisateurs du système de messagerie peuvent envoyer et recevoir des messages personnels internes et externes. Toutefois, cet usage ne doit pas perturber leur travail ni celui d'autrui, ni entraver l'exercice de leurs fonctions et responsabilités. Tout usage excessif de la messagerie à des fins personnelles est à éviter. Le système de messagerie ne peut être utilisé pour des activités professionnelles privées ni pour divulguer, diffuser ou transmettre de quelque manière que ce soit des informations confidentielles appartenant à l'entreprise.

4.4. Contenu :

Tous les courriels, qu'ils soient explicites ou implicites, doivent être exempts de toute référence sexuelle, raciale ou religieuse, de toute mention de crime ou de harcèlement, et doivent être rédigés dans un langage acceptable pour la communication professionnelle en milieu de travail.

4.5. Confidentialité :

La confidentialité des messages électroniques n'est pas garantie. Tout message envoyé ou reçu peut être consulté par des collègues autres que le destinataire, que ce soit accidentellement (par exemple, en laissant une session informatique ouverte) ou intentionnellement (par exemple, en ouvrant un courriel pour diagnostiquer des problèmes de connexion). Par conséquent, les messages ne peuvent être considérés comme privés ou confidentiels. Les messages personnels doivent être rédigés en tenant compte de la possibilité qu'ils soient consultés par des tiers. Quant aux courriels externes, ils sont par nature non sécurisés et peuvent être interceptés et lus par des tiers à notre insu. Les messages présentant un niveau de confidentialité ou de sensibilité particulier doivent être envoyés par un autre moyen et selon les méthodes spécifiées dans la Politique de sécurité des informations et de transfert de données.

4.6. Pièces jointes :

Afin d'empêcher la diffusion de contenu inapproprié sur le réseau de l'entreprise et de réduire les risques d'infection virale, les pièces jointes (images, textes ou feuilles de calcul) des courriels ne peuvent être téléchargées que si elles proviennent de sources fiables (c'est-à-dire de contacts dont vous connaissez l'identité) et ne contiennent aucun contenu inapproprié. Les fichiers exécutables joints aux courriels ne doivent pas être ouverts. Dans ce cas, veuillez les transmettre au responsable informatique pour avis. Les extensions de fichiers exécutables incluent : .EXE, .COM, .VBS, .SCR, game.exe et screen.scr.

4.7. Chaînes de lettres/blagues :

Les chaînes de lettres et les messages humoristiques constituent une utilisation inappropriée du temps des employés et des ressources de l'entreprise, et peuvent involontairement offenser le destinataire. Ces messages ne doivent pas être transférés à d'autres utilisateurs et doivent être supprimés du réseau dès leur réception.

4.8. Fausses alertes de virus :

Les messages provenant de sources externes et contenant des alertes antivirus ne doivent pas être transférés. En pratique, la plupart de ces messages sont infondés. Toutefois, il convient de les supprimer de la boîte de réception après avoir contacté l'assistance informatique et obtenu ses conseils.

4.9. Utilisation de systèmes de messagerie externes pour les transactions de l'entreprise :

Toute correspondance par courriel relative aux activités et transactions de l'entreprise doit être envoyée via le réseau de messagerie de l'entreprise. L'utilisation de systèmes et comptes de messagerie personnels (par exemple, AOL, Hotmail, services de messagerie fournis par les fournisseurs d'accès Internet et tout autre service non mentionné ici) à des fins professionnelles est interdite. Les employés devant accéder au réseau de l'entreprise en dehors des locaux de l'entreprise sont invités à contacter l'équipe d'assistance informatique pour obtenir des conseils sur le télétravail.

4.10. Consignes pour l'envoi de courriels :

4.10.1. Identification des destinataires des courriels :

a) Vérifiez attentivement : Pour éviter les erreurs courantes d'envoi d'e-mails, telles que l'utilisation incorrecte des icônes « Répondre à tous » et « Répondre », les adresses des destinataires doivent être soigneusement vérifiées avant l'envoi des e-mails.

b) Destinataire principal : Outre l'adresse du destinataire principal indiquée dans l'en-tête du courriel, l'objet du message doit être « Message à xxxx » ou « Cher/Chère M./Mme xxxx » afin d'indiquer clairement le destinataire et la personne qui est censée répondre. Les destinataires en copie (CC) doivent être mis en copie à titre informatif uniquement. Lors de l'envoi d'un courriel, il est nécessaire d'ajouter un destinataire en copie (CC).

La personne que vous ajoutez au champ CC est une personne que vous souhaitez informer, même si elle n'est pas le destinataire direct du courriel. Si vous ajoutez une personne en copie, elle sera visible par tous les destinataires du courriel. Autrement dit, en ajoutant quelqu'un en copie, vous indiquez qu'il aura connaissance du courriel.

c) Listes de destinataires en copie (CC) : De même qu'il convient de bien réfléchir aux destinataires et à la liste des destinataires en copie d'une note ou d'une lettre, il est important d'être tout aussi vigilant lors de la rédaction d'un courriel. En particulier, il faut éviter d'utiliser plusieurs listes de destinataires en copie. Une analyse approfondie doit être menée afin de déterminer si la mise en copie d'informations ou la demande d'avis de chaque personne concernée est justifiée et pertinente. Les listes de destinataires en copie ne doivent pas être utilisées pour les courriels adressés à des groupes de clients ; ces communications doivent être envoyées via le portail. Il est essentiel d'éviter d'utiliser des listes d'adresses électroniques dans les champs « À » ou « Cc » afin de respecter la confidentialité des destinataires.

d) Liste CCI : « CCI » signifie « Copie carbone fermée ». L'adresse électronique saisie dans ce champ recevra le message. Les destinataires des champs « À » et « Cc » ne peuvent pas voir les adresses électroniques saisies dans ce champ. Seuls l'expéditeur et le destinataire dont l'adresse électronique est saisie dans ce champ peuvent voir cette information. En revanche, les personnes dont le nom est saisi dans le champ « CCI » peuvent voir les destinataires des champs « À » et « Cc ».
Bien que la fonction CCI (copie cachée) puisse être appropriée dans les courriels envoyés à des tiers, il est déconseillé de ne pas divulguer d'informations confidentielles à une ou plusieurs personnes dans le cadre de communications professionnelles. En effet, les courriels peuvent être transférés ultérieurement, risquant ainsi de divulguer des informations confidentielles. Des problèmes de confiance peuvent survenir lorsque des messages considérés comme privés sont partagés de cette manière ; par conséquent, il est généralement préférable d'éviter la fonction CCI entre collègues.

e) Envoi d'e-mails en masse : L'envoi d'e-mails en masse ne doit être utilisé qu'à des fins professionnelles. Il ne peut en aucun cas servir à l'envoi de messages individuels.
En outre, la promotion ou la recommandation des biens et services de tiers est également inappropriée.

f) Envoi de pièces jointes (documents/tableurs) : Vous pouvez utiliser le courrier électronique pour diffuser des notes de rappel ou d'autres pièces jointes. Cependant, il est déconseillé d'envoyer par courrier électronique des fichiers et pièces jointes de plus de 10 Mo. L'équipe d'assistance informatique peut vous conseiller sur l'envoi de fichiers volumineux via des solutions telles que le stockage partagé.

5. PROTECTION DES DONNÉES PERSONNELLES :

Toute communication contenant des données personnelles sera soumise à la législation applicable en matière de protection des données. Consultez la politique de notre entreprise en matière de traitement et de protection des données personnelles et…

La politique de sécurité de l'information contient des informations détaillées sur la manière dont les données personnelles seront protégées et chaque employé doit en prendre connaissance.