



MESSAGERIE ÉLECTRONIQUE
PROCÉDURE D'UTILISATION ET
RÉGLEMENTATION RELATIVE À SES PRINCIPES

KVKK_Y5 VERSION 1.00

1. INTRODUCTION, OBJECTIFS ET DÉFINITIONS

- 1.1. Les applications de communication électronique, telles que la messagerie électronique et l'agenda, sont des outils de communication essentiels pour la Société et contribuent largement à la réalisation de ses activités. Le présent règlement vise à définir les procédures et les principes relatifs à l'utilisation acceptable des applications de communication électronique utilisées dans le cadre des activités de la Société, notamment ses activités économiques, de recherche et de services administratifs. Il détaille également la sécurité de ces applications et la protection des données personnelles qui y sont traitées, ainsi que la réglementation applicable.
- 1.2. La société Kardelen Paint and Chemical Industry Trade Limited utilise le service Microsoft Office 365, notamment le logiciel « Office » utilisé par ses employés, comme système de communication électronique. Le présent règlement définit les directives à suivre concernant l'utilisation des systèmes de communication électronique au sein de la société, y compris, mais sans s'y limiter, Outlook et Skype Entreprise.
- 1.3. Dans le présent règlement, le terme « message » désigne toute communication écrite envoyée, reçue ou publiée au moyen d'un logiciel de communication électronique, y compris les documents, enregistrements, images ou autres fichiers joints.

2. SÉCURITÉ

- 2.1. L'accès au contenu de tous les comptes de messagerie est soumis aux motifs raisonnables décrits à la section 11.9 « Conditions d'utilisation acceptable des ressources informatiques (Politique d'utilisation acceptable) » du Règlement de la Société sur la surveillance des communications électroniques et la Politique de sécurité des données et des informations électroniques.
- 2.2. La messagerie électronique et les calendriers ne sont pas des services à sécurité garantie. Par exemple, des personnes non autorisées peuvent surveiller la transmission des courriels ou des événements du calendrier, ou envoyer des courriels frauduleux en usurpant l'identité d'un utilisateur. Par conséquent, les utilisateurs ne doivent inclure aucune information confidentielle ou personnelle dans leurs messages électroniques, sauf si cette information est chiffrée. La protection de la sécurité des données personnelles ou sensibles est une obligation impérative lors du partage d'informations. L'entreprise et ses employés ont des obligations légales, éthiques et morales de protéger la sécurité et la confidentialité des données sensibles lors de leur collecte, traitement, stockage et transfert. Chaque donnée considérée comme sensible doit être protégée par des méthodes de chiffrement appropriées. Lors du transfert de telles données, il est nécessaire de consulter l'équipe de support informatique concernant la protection de la confidentialité et de la vie privée, et les règles générales stipulées dans la politique de sécurité des transferts de données doivent toujours être respectées.

2.3. Afin d'améliorer la collaboration entre nos employés, les événements du calendrier comportant un objet peuvent être rendus visibles par défaut aux autres membres du personnel. Par conséquent, il est demandé à tous les employés de s'abstenir d'inclure des informations sensibles (notamment des données personnelles) dans l'objet de leurs événements.

Les notes d'une entrée de calendrier, y compris les pièces jointes, sont invisibles par défaut pour les autres. Toutefois, il convient d'éviter d'inclure des données sensibles ou personnelles dans les entrées de calendrier, conformément aux principes énoncés dans la section 1. Veuillez consulter les sections pertinentes de la Politique de sécurité de l'information et de la Politique de protection des données personnelles de notre entreprise concernant les données sensibles et les catégories particulières de données personnelles qui doivent rester confidentielles. Veuillez également noter que d'autres informations personnelles peuvent être considérées comme sensibles selon les circonstances, telles que les noms des participants aux réunions ou les types d'autorisations (rendez-vous médicaux, urgences familiales, etc.). Pour masquer l'objet des entrées de calendrier privées, il suffit de sélectionner l'icône de cadenas.

2.4. Les comptes de messagerie professionnelle de l'entreprise sont accessibles de partout via l'**application web Outlook**, depuis n'importe quel navigateur. Lorsque vous utilisez l'application web Outlook, votre session expire automatiquement après une heure d'inactivité afin d'empêcher tout accès non autorisé à votre compte. Passé ce délai, le système vous invite à vous réauthentifier en saisissant votre nom d'utilisateur et votre mot de passe.

2.5. Les utilisateurs doivent faire preuve de vigilance lors de la rédaction de leurs courriels et tenir compte du fait que la fonction de saisie automatique peut suggérer une adresse électronique différente de celle prévue. Si des données personnelles ou professionnelles sensibles, ou des données à caractère personnel relevant de catégories particulières, sont envoyées à une adresse électronique erronée, la violation de données potentielle ou avérée doit être immédiatement signalée aux parties concernées et consignée au moyen du formulaire prévu par le Règlement relatif au plan de réponse aux violations de données à caractère personnel.

3. ARCHIVAGE, DURÉE DE CONSERVATION ET SUPPRESSION

3.1. Tous les messages datant de plus de deux ans seront automatiquement déplacés vers des dossiers d'archives pour les nouveaux utilisateurs. Pour rechercher des courriels datant de plus de deux ans, les utilisateurs devront se rendre dans la section « Archives en ligne ». Pour modifier ce paramètre, sélectionnez l'une des options suivantes via l'option « Attribuer une stratégie » du menu « Accueil » :

- Archivage (Tous les messages électroniques sont stockés dans les dossiers par défaut d'Outlook (par exemple, (Les éléments de la boîte de réception et les éléments envoyés) seront conservés et ne seront pas archivés automatiquement.
- Archiver les courriels datant de plus de 2 ans.

3.2. Les messages électroniques ne sont normalement jamais supprimés. Les utilisateurs de messagerie professionnelle peuvent choisir parmi les options suivantes : • Supprimer les messages de plus de 5 ans •

Supprimer les messages de plus de 10 ans

• Stocker tous les messages indéfiniment

3.3. Si l'une des options de « suppression » mentionnées ci-dessus est sélectionnée, les messages plus anciens que la période sélectionnée par l'utilisateur seront automatiquement supprimés sans autre avertissement.

3.4. En cas de cessation d'activité d'un employé au sein de l'entreprise, son compte sera désactivé progressivement, c'est-à-dire qu'il sera désactivé à la date de son départ. Le compte de messagerie ne sera plus accessible. Six mois après cette date, les comptes seront définitivement supprimés, puis la boîte mail sera entièrement vidée 30 jours plus tard. Les employés concernés peuvent demander à conserver leur identifiant et leur compte de messagerie professionnels pendant une durée maximale de six mois afin d'assurer la continuité des activités de l'entreprise. Dans ce cas, l'autorisation sera accordée sur demande des responsables de service et du responsable informatique.

3.5. Conformément à la politique de l'entreprise, les responsables de service peuvent accéder aux courriels et aux fichiers des employés après leur départ afin d'assurer la continuité des activités. Il est donc conseillé aux employés dont le contrat de travail est résilié de supprimer tous leurs courriels et fichiers personnels avant leur départ.

4. UTILISATION D'ADRESSES E-MAIL AUTRES QUE LE COMPTE E-MAIL PROFESSIONNEL DE L'ENTREPRISE ET LE TRANSFERT D'E-MAIL

4.1. Afin de garantir la sécurité et la fiabilité des communications par courriel, les employés de la Société disposent d'adresses courriel professionnelles et bénéficient d'une garantie de réception des courriels. Cette garantie ne s'applique pas si les employés utilisent une adresse courriel externe (non professionnelle) pour leurs communications professionnelles et transfèrent automatiquement les courriels officiels de l'entreprise vers cette adresse externe. Par conséquent, l'utilisation d'une adresse courriel externe pour les activités et transactions professionnelles de la Société, ainsi que le transfert automatique vers des adresses courriel externes (non professionnelles), sont interdits.

4.2. Les employés qui estiment avoir une raison valable de transférer le courriel professionnel de leur entreprise vers un compte de courriel externe doivent signaler cette demande au service informatique.

5. AUTRES QUESTIONS

5.1. L'accès à la messagerie électronique est exclusivement réservé aux besoins de ses activités et transactions officielles. Tout accès à la messagerie à des fins personnelles, occasionnelles ou non, est interdit.

Ce type d'utilisation est autorisé tant qu'il n'interfère pas avec les opérations de la Société, ne distraie pas l'employé (en termes de volume ou de fréquence) ou n'empêche pas d'autres personnes d'accéder au réseau pour mener des activités et des transactions officielles de la Société.

5.2. Les représentants syndicaux qui sont des employés de l'entreprise peuvent utiliser le système de messagerie électronique pour communiquer avec les membres du syndicat et pour mener des activités et des affaires syndicales.

5.3. Il est conseillé à tous les employés de télécharger une nouvelle photo d'eux-mêmes comme icône afin d'être facilement reconnaissables par les autres utilisateurs de l'environnement Microsoft Office 365. Toutefois, si un employé choisit de ne pas partager sa photo publiquement, il ne doit pas utiliser une photo autre que son reflet, ou bien le logo de l'entreprise doit être défini comme icône par défaut.

5.4. En utilisant les systèmes de communication électronique fournis par la Société, les utilisateurs reconnaissent que celle-ci ne garantit pas la confidentialité des messages ou données stockés ou transmis par ces systèmes ; que la Société se réserve les droits énoncés dans le présent document ; et que l'utilisation de ces systèmes est limitée aux fins approuvées par la Société, lesquelles leur ont été notifiées. L'utilisation des systèmes de communication électronique de la Société dans le cadre de ses activités et à des fins personnelles non essentielles n'est pas un droit, mais une autorisation accordée à ses employés et aux tiers autorisés. Par conséquent, la Société peut, à tout moment et sans préavis, bloquer l'accès à tout ou partie de ses systèmes de communication électronique et informatiques (pour tous les utilisateurs ou certains d'entre eux). Les utilisateurs des systèmes de communication électronique et informatiques de la Société sont tenus de respecter le Règlement de la Société relatif aux procédures et principes d'utilisation appropriée d'Internet et des outils de communication électronique, ainsi que les Conditions d'utilisation acceptables (Politique d'utilisation acceptable). En utilisant ces systèmes, les utilisateurs reconnaissent avoir pris connaissance de la Politique d'utilisation acceptable et s'engagent à la respecter. Ils consentent également à sa mise en œuvre par la Société. Les utilisateurs s'engagent en outre à respecter la législation applicable et à s'abstenir de tout comportement susceptible d'engager la responsabilité de la Société. La Société se réserve le droit de modifier à tout moment et sans préavis le Règlement relatif aux procédures et principes d'utilisation appropriée d'Internet et des outils de communication électronique, ainsi que toute autre condition d'utilisation des systèmes informatiques, et de prendre toute mesure requise ou appropriée conformément à la législation applicable.

5.5. La Société doit protéger l'intégrité de ses systèmes de communication électronique internes et de ses systèmes informatiques ainsi que leurs utilisateurs contre toute utilisation non autorisée ou inappropriée de ces installations et contre toute violation des règles et politiques de la Société.

Afin d'identifier les utilisations susceptibles d'entraîner des infractions, la Société se réserve le droit de restreindre ou de bloquer l'accès à ses services à toute personne, sans préavis, et de rechercher, copier, supprimer ou modifier toute donnée, tout fichier ou toute ressource système pouvant nuire à l'utilisation prévue des systèmes informatiques ou servir à enfreindre les règles ou politiques de la Société. La Société se réserve également le droit d'effectuer des contrôles périodiques de ses systèmes informatiques afin d'assurer leur protection et le respect de ses droits. Ces contrôles incluent, par exemple, l'analyse des courriels traités sur les ordinateurs et serveurs de la Société à la recherche de logiciels malveillants.

5.6. La société n'est pas responsable de toute perte de données ou interférence avec les fichiers qui pourrait survenir en raison de dysfonctionnements du système ou d'autres raisons liées au travail qu'elle effectue pour assurer la confidentialité et la sécurité des systèmes en question.

5.7. Les utilisateurs ne sont autorisés à autoriser personne à utiliser leurs comptes professionnels, quel qu'en soit le motif. Le titulaire du compte est responsable de toute utilisation de celui-ci. Les utilisateurs doivent prendre toutes les précautions raisonnables, notamment la protection du mot de passe et des documents, afin d'empêcher toute utilisation non autorisée de leurs comptes. Ils ne doivent communiquer leur mot de passe à personne et doivent le modifier régulièrement. Le titulaire du compte est responsable de toute transaction effectuée à l'aide d'un mot de passe associé à un compte utilisateur, même si l'auteur de la transaction n'est pas le titulaire du compte.

5.8. Aucun système de communication électronique ou informatique appartenant à l'entreprise ne peut être utilisé de manière irresponsable ou de façon à perturber le travail d'autrui. Ceci inclut : la transmission ou la mise à disposition de contenus diffamatoires, injurieux ou harcelants, de chaînes de lettres, d'envois de masse non autorisés ou de publicités non sollicitées ; l'endommagement intentionnel, par imprudence ou par négligence, d'un système, de matériel ou d'informations n'appartenant pas à l'utilisateur ; la perturbation intentionnelle des communications électroniques ou toute autre atteinte à la vie privée d'autrui ou l'accès à des informations qui n'appartiennent pas à l'utilisateur ou qui ne lui sont pas destinées ; l'utilisation abusive intentionnelle des ressources système ou le fait d'inciter autrui à les utiliser de manière abusive ; ou le téléchargement de logiciels ou de données sur les systèmes administratifs à partir de sources non fiables telles que les logiciels libres.

5.9. La société décline toute responsabilité quant au contenu qu'elle ne diffuse pas elle-même par courriel ou autres moyens de communication. L'accès au contenu fourni par des tiers se fait aux risques et périls de l'utilisateur, qui reconnaît pouvoir le juger offensant, inapproprié ou choquant. Les services de messagerie et les systèmes informatiques sont fournis « EN L'ÉTAT » et « SELON DISPONIBILITÉ ». La société présume que le contenu tiers est exact, complet et fiable.

L'utilisateur se dégage de toute responsabilité à cet égard. Il est responsable des informations qu'il détient ou stocke dans ses systèmes de messagerie.

5.10. L'Utilisateur reconnaît que (i) toute tentative visant à entraver le fonctionnement du courrier électronique et d'autres systèmes de communication ou leur utilisation par d'autres ; (ii) le téléchargement de contenu qui surcharge le courrier électronique et d'autres systèmes de communication électronique ; (iii) les actions qui mettent en danger la sécurité générale des systèmes de communication électronique et/ou nuisent aux autres utilisateurs ; (iv) l'utilisation ou la tentative d'utilisation de logiciels qui entravent ou perturbent le fonctionnement du courrier électronique et d'autres systèmes de communication sont absolument interdites.

une En cas de violation du présent règlement par un tiers, ou en cas d'information concernant erreur ou un contournement relatif à la sécurité des courriels et autres systèmes de communication électronique, il est obligatoire de signaler immédiatement l'incident au service informatique.

5.12. Toute utilisation non autorisée ou inappropriée de la messagerie électronique et des autres systèmes de communication électronique de l'entreprise, y compris le non-respect des dispositions du présent règlement, constitue une violation de la politique de l'entreprise et requiert des mesures disciplinaires approuvées par le directeur général.

6. RÉVISION

Le directeur général adjoint est chargé de la révision et de la mise à jour de ce document. Les modifications et mises à jour sont publiées après approbation de la direction générale. La révision a lieu chaque année en juin.

