SÉCURITÉ DE L'INFORMATION

POLITIQUE

KVKK_P5 VERSION 1.00

KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED COMPANY

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

1. Objectif :

L'information joue un rôle fondamental dans le soutien de toutes les activités de Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi. La sécurisation adéquate de toutes les informations traitées par notre entreprise est essentielle au succès de nos opérations économiques et administratives. Cet objectif sera atteint en abordant trois aspects fondamentaux de la sécurité de l'information : la confidentialité, l'intégrité et l'accessibilité des données, qui constituent des éléments essentiels à la protection des informations de l'entreprise.

Les objectifs de cette politique sont les suivants :

1.1. Les ressources informationnelles de l'entreprise sont adéquatement protégées contre la perte, l'utilisation abusive et les violations.
assurer un niveau de protection ;

1.2. Tous les utilisateurs acceptent la présente politique et les autres documents de politique et codes de conduite connexes.
et de veiller à ce qu'ils soient informés des directives ;

1.3. Tous les utilisateurs sont soumis à la loi turque applicable et à leurs obligations dans ce contexte.
pour s'assurer qu'ils sont conscients de leurs responsabilités ;

1.4. Sensibiliser les employés et les autres parties prenantes à la nécessité de mettre en œuvre des mesures de sécurité appropriées dans toute l'entreprise dans le cadre de l'objectif d'assurer et de soutenir efficacement la sécurité de l'information ;

1.5. S'assurer que tous les utilisateurs sont conscients de leurs responsabilités en matière de confidentialité, d'intégrité et de disponibilité des données qu'ils traitent ;

La présente politique doit être considérée conjointement avec la politique de traitement et de protection des données personnelles de Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi et les principes de mise en œuvre connexes, qui contiennent des informations détaillées sur la protection des données personnelles.

2. CHAMP D'APPLICATION :

Cette politique couvre la protection des actifs informationnels électroniques obtenus à partir des activités commerciales menées au sein de la Société et des activités connexes de logistique, d'entreposage, de comptabilité, de finance, d'assurance qualité, d'achat, de ressources humaines, juridiques, de vente, de marketing, d'audit interne et de traitement de l'information, ainsi que les processus de sécurité de l'information utilisés par Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi pour assurer le traitement, le stockage, la protection, la confidentialité et l'intégrité des données personnelles détenues au sein de la Société conformément à la loi.

2.1. Tous les employés de la Société et toutes les autres personnes tierces concernées, y compris les invités autorisés à accéder aux informations contrôlées par ou pour le compte de la Société, sont tenus de respecter la Politique de sécurité de l'information et les principes de mise en œuvre associés, tels qu'ils sont énoncés dans le présent document. Les dispositions de cette Politique couvrent les procédures par lesquelles les personnes susmentionnées accèdent et utilisent toutes les données et tous les logiciels appartenant à la Société ou dont elle détient la licence d'utilisation, que ce soit par connexion directe ou indirecte aux réseaux fournis par Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi, par le biais d'appareils appartenant à la Société, loués par elle ou mis à sa disposition, ou par l'utilisation de tous les autres outils et systèmes externes, aussi bien au sein de la Société que par le biais de systèmes externes.

2.2. La présente politique s'applique à toutes les données détenues par la Société, qu'elles soient électroniques ou physiques, y compris les méthodes énumérées ci-dessous :

- Données électroniques stockées et traitées par les ordinateurs de bureau et portables et autres appareils, ainsi que par les périphériques de stockage ;
- Données transmises via des environnements réseau ;
- Informations transmises par fax ou par des méthodes de transmission similaires ;
- Tous les documents papier ; • Les documents visuels et photographiques, y compris les microfiches, les diapositives et les enregistrements de vidéosurveillance ; les données audio relatives aux messages vocaux et aux conversations enregistrées, y compris les communications en face à face ;

2.3. Les données de l'entreprise peuvent généralement être classées en données personnelles et données non personnelles :

- Les données personnelles sont traitées conformément à la politique de traitement et de protection des données personnelles de la société et sont soumises au plus haut niveau de protection ;
- Les données non personnelles comprennent les types de données suivants :
  - je. Catégories particulières de données de l'entreprise, notamment les données de planification commercialement sensibles, les données de recherche, les données protégées par des accords de confidentialité et les données légalement désignées comme privilégiées ou confidentielles. Les données de cette catégorie bénéficient d'un niveau de protection élevé.
  - ii. Les données de l'entreprise rendues publiques par leur publication sur son site web ou conformément à la réglementation en vigueur, notamment la loi sur la liberté d'information, doivent impérativement être exactes, à jour et protégées contre toute perte ou accès non autorisé.

2.4. Les dispositions de la présente politique s'appliquent à toutes les étapes du cycle de vie des données, y compris la collecte, le stockage, le traitement et la destruction des données.

2.5. Bien que l'utilisation des plateformes de médias sociaux par nos employés soit libre et non directement réglementée par la Société, notre Société attend de ses employés qu'ils se conforment aux dispositions de la présente politique et qu'ils s'abstiennent de toute action susceptible de nuire à la réputation de l'entreprise.

Elle exige que les individus s'abstiennent de tels comportements. Pour plus d'informations à ce sujet, veuillez consulter la Politique relative aux médias sociaux.

3. RESPONSABILITÉS ET AUTORITÉ :

Les responsabilités et les pouvoirs des employés sont définis dans leurs fiches de poste, de même que leurs qualifications et compétences. Les responsabilités des unités et du personnel concernés en matière de maintien et d'amélioration des activités de sécurité de l'information sont les suivantes :

3.1. Chefs de département

Les chefs de département sont responsables de veiller à ce que le personnel et les autres personnes autorisées employées dans les unités placées sous leur supervision respectent les procédures et les principes, en particulier ceux énoncés dans les conditions d'utilisation des ressources informatiques.
Ils sont également chargés d'enregistrer les ressources informationnelles détenues par les unités qu'ils supervisent dans l'inventaire des ressources informationnelles de l'entreprise et d'attribuer un utilisateur de ressource informationnelle à chaque ressource informationnelle.

3.2. Utilisateurs des ressources d'information

Les utilisateurs responsables des ressources d'information sont les personnes désignées pour chaque ressource d'information répertoriée dans l'inventaire des ressources d'information de l'entreprise. Ils sont chargés de réaliser annuellement une évaluation des risques liés à la protection des données en analysant les risques pour la sécurité et la confidentialité des ressources d'information dont ils ont la responsabilité, et de mettre en œuvre les mesures appropriées.

3.3. Nos employés et les tiers autorisés

Tous les employés de la Société et toutes les personnes autorisées par celle-ci à accéder aux ressources d'information sont tenus de respecter les dispositions de la présente Politique. Avant d'utiliser leur identifiant, conformément aux Conditions d'utilisation des ressources informatiques, chaque employé doit accepter les conditions générales d'utilisation qui s'afficheront à l'écran. En cas de divulgation ou de perte accidentelle de données, d'accès non autorisé, de virus informatique, de logiciel malveillant ou de tout autre incident compromettant la sécurité des informations, ou en cas de suspicion de tels incidents, la situation doit être immédiatement signalée au Responsable informatique. Les personnes concernées peuvent contacter directement le Responsable informatique ou ses collaborateurs à cet effet. (Voir la section 7.1 pour les coordonnées.)

3.4. Responsable informatique

Le responsable informatique est chargé de superviser les ressources en technologies de l'information et de la communication et de mener les activités quotidiennes liées à la sécurité de l'information. Le responsable informatique peut auditer tous les systèmes utilisés afin d'identifier et d'atténuer les risques de sécurité, ou supprimer ou désactiver les noms d'utilisateur/de connexion, les données et/ou les programmes jugés non sécurisés sur les systèmes situés sur le réseau.

4. RESPECT DE LA LÉGISLATION APPLICABLE

4.1. La société Kardelen Paint and Chemical Industry Trade Limited est tenue de respecter toutes les lois et réglementations administratives turques applicables. En matière de sécurité de l'information, les principaux textes législatifs sont la loi n° 5651 relative à la réglementation des publications sur Internet et à la lutte contre les infractions commises par le biais de ces publications, la loi n° 6698 relative à la protection des données personnelles et le règlement relatif à la sécurité des réseaux et de l'information dans le secteur des communications électroniques.

4.2. Le respect des dispositions légales susmentionnées est de la responsabilité de tous les utilisateurs, et leur responsabilité individuelle peut être engagée en cas de non-respect. Si un employé agit contrairement à la présente politique ou aux dispositions de la législation applicable, des mesures disciplinaires pourront être prises conformément au contrat de travail signé avec notre société et au règlement disciplinaire en vigueur. Le non-respect de ces dispositions par nos fournisseurs ou sous-traitants peut entraîner la résiliation de leur contrat. Dans certains cas, des poursuites judiciaires pourront être engagées.

5. INVENTAIRE DES DONNÉES DE L'ENTREPRISE ET IMPACT DE LA PROTECTION DES DONNÉES ÉVALUATION

5.1. La société Kardelen Paint and Chemical Industry Trade Limited tient un inventaire des données recensant les sources de données utilisées au sein de son organisation. Les chefs de service et les directeurs d'agence sont chargés de désigner un utilisateur pour chaque source d'information gérée par leur unité respective et d'enregistrer cette information dans l'inventaire des données de l'entreprise.

5.2. Une analyse d'impact sera réalisée annuellement pour toutes les sources d'information utilisées, concernant les risques pour la confidentialité et la sécurité des données, ainsi que les risques que les outils utilisés peuvent engendrer pour le droit à la vie privée des personnes. Une analyse d'impact sera également réalisée avant l'utilisation de nouvelles sources d'information. Les mesures décidées pour atténuer ces risques pour les sources traitant des données classées comme données sensibles seront précisées dans l'inventaire des données.

6. SURVEILLANCE DES COMMUNICATIONS ÉLECTRONIQUES

Conformément à l'article 6 de la loi n° 5561 relative à la réglementation des publications sur Internet et à la lutte contre les infractions commises par le biais de ces publications, intitulé « Obligations du fournisseur d'accès », la Société prend les mesures nécessaires pour stocker les informations relatives au trafic de communications électroniques qu'elle reçoit ou envoie, dans la limite des finalités prévues par la loi, et pour garantir l'exactitude, l'intégrité et la confidentialité de ces informations. Ces mesures comprennent notamment la surveillance de toute utilisation non autorisée ou à des fins criminelles des informations, la réalisation d'audits et d'interventions pour protéger le système contre les menaces telles que les virus, le piratage et les attaques par déni de service, ainsi que la garantie de la conformité des opérations informatiques avec les politiques et directives de la Société.

Ces procédures ne sont pas exhaustives. Les inspections seront effectuées conformément aux principes de mise en œuvre relatifs aux communications électroniques et à l'examen des données.

7. ÉVÉNEMENTS LIÉS À LA SÉCURITÉ DES DONNÉES

7.1. Si un utilisateur détecte ou soupçonne une violation de la sécurité des données ou une utilisation abusive des ressources d'information qui viole la confidentialité, l'accessibilité et l'intégrité des données, il en informera l'équipe de support du département informatique.

7.2. Si une violation de la sécurité des données implique la destruction, la perte, l'altération, l'accès inefficace ou la divulgation accidentelle ou illicite de données personnelles à des tiers non autorisés, les utilisateurs doivent immédiatement préparer et envoyer le rapport de notification de violation de la sécurité des données, inclus en annexe au plan de réponse aux violations de données, au responsable/gestionnaire de la protection des données.

Coordonnées du responsable/directeur de la protection des données :
Kardelen Paint and Chemical Industry Trade Limited Company
Téléphone : +90 312 398 11 33
Télécopie : +90 312 398 09 11
Courriel : kvkk@kardelenboya.com.tr

7.3. En cas d'incident de sécurité des données, ou lorsqu'un tel incident est suspecté de se produire, le responsable informatique peut prendre rapidement des mesures pour résoudre l'incident ou atténuer les dommages potentiels, comme le blocage de l'accès des utilisateurs au système ou l'inspection des appareils connectés au réseau.

7.4. Le refus de signaler un incident de sécurité des données ou une violation de données personnelles peut entraîner une enquête disciplinaire. En cas d'hésitation à signaler un incident, il est possible de consulter le responsable informatique ou le délégué à la protection des données.

8. FORMATION À LA SÉCURITÉ DES DONNÉES

8.1. Les employés qui utiliseront du matériel informatique pour la première fois, ainsi que les tiers autorisés à y accéder, doivent connaître les politiques et procédures de sécurité de l'information de l'entreprise. De plus, avant d'obtenir l'accès aux services informatiques, les utilisateurs doivent être formés aux exigences de sécurité liées à leur travail et, plus généralement, à la bonne utilisation du matériel informatique de l'entreprise. Il incombe aux responsables de veiller à ce que les employés soient correctement formés et que les dossiers de formation soient conservés. Les utilisateurs doivent être informés de la présente politique, notamment des procédures de signalement décrites à la section 7.

8.2. Tous les employés de l'entreprise suivront une formation de sensibilisation à la sécurité de l'information et à la protection des données personnelles, dispensée en ligne ou en présentiel. Il est prévu que ces formations deviennent obligatoires à l'avenir.

9. ÉVALUATIONS DE SÉCURITÉ DANS LE DOMAINE DE L'EMPLOI

9.1. Les rôles et responsabilités à assumer en matière de sécurité, tels que spécifiés dans la présente politique et les réglementations connexes, doivent être inclus dans les descriptions de poste, le cas échéant.
Ces responsabilités devraient inclure les responsabilités générales relatives à la mise en œuvre de la politique de sécurité, ainsi que les responsabilités relatives à la protection d'actifs informationnels spécifiques ou à l'exécution de processus ou d'activités de sécurité.

9.2. Étant donné que l'autorité et les responsabilités en matière de sécurité des données peuvent changer en cas de candidatures ou de changements d'emploi des employés, ces questions doivent être évaluées par les Ressources Humaines.

9.3. Les employés des fournisseurs ou des sous-traitants et les utilisateurs tiers qui utiliseront les systèmes d'information de la Société seront tenus de signer des accords de confidentialité dans le cadre de leurs contrats, et s'ils ont accès à des données personnelles détenues par la Société, ils seront tenus de signer des accords de partage de données.

10. PROTECTION DES DONNÉES DE CATÉGORIE SPÉCIALE

La mise en œuvre de l'article 10.1 est essentielle. L'entreprise a mis en place des mesures de sécurité renforcées pour protéger les données personnelles sensibles.

10.2. Les données de catégories particulières ne doivent pas être stockées ni transmises via des adresses électroniques individuelles (Gmail, Hotmail, etc.) ou des services de stockage « cloud » en ligne (Google Apps, Dropbox, etc.) qui ne sont pas fournis par la Société.

Les bases de données et les ordinateurs contenant des données sensibles doivent être cryptés et exiger que les utilisateurs saisissent des identifiants pour accéder aux données (Article 10.3).
Dans la mesure du possible, les données doivent être anonymisées ou pseudonymisées afin de protéger les identités, notamment lorsqu'il s'agit de données identifiables de patients/participants.

10.4. Toutes les données sur les appareils utilisés par mon entreprise doivent être effacées de manière sécurisée lorsqu'ils sont mis au rebut.

10.5. Les fichiers de données doivent être chiffrés à la fois sur le support où ils sont stockés et pendant leur transmission.

11. CONDITIONS D'UTILISATION DES RESSOURCES INFORMATIQUES

Toute personne utilisant les ressources informatiques de l'entreprise est réputée avoir accepté ce qui suit : 11.1.

Les ressources informatiques désignent l'ensemble du matériel, des logiciels, des services et des ressources fournis pour le fonctionnement de l'entreprise. Cela inclut tous les réseaux informatiques, les connexions câblées, etc.

ou les ordinateurs sans fil, les imprimantes, les appareils mobiles, les périphériques de stockage, les systèmes audiovisuels et les services cloud sont considérés comme faisant partie des ressources informatiques.

11.2. Chaque utilisateur doit comprendre et mettre en œuvre les conseils donnés concernant l'utilisation sécurisée des ressources informatiques, participer à une formation de sensibilisation à la sécurité de l'information et se familiariser avec la déclaration de sensibilisation à la sécurité de l'information ; 11.3.

L'utilisation des ressources informatiques de l'entreprise et leur utilisation pour donner accès à des ressources externes doivent se limiter à la recherche, à la formation, aux tâches administratives et aux autres utilisations autorisées et nécessaires au fonctionnement de l'entreprise. L'utilisation des ressources informatiques à des fins personnelles sans autorisation préalable est interdite. 11.4. Les activités menées pour le compte de l'entreprise doivent être réalisées exclusivement à l'aide des outils de traitement de l'information fournis par celle-ci. Le recours à des services informatiques externes pour les activités de l'entreprise expose les données de celle-ci à des risques et est donc interdit, sauf justification suffisante. Par exemple, il convient d'utiliser la messagerie électronique de l'entreprise plutôt que Dropbox, OneDrive ou des services de messagerie tels que Gmail et Hotmail. 11.5.

L'utilisation des ressources informatiques de l'entreprise à des fins personnelles est autorisée uniquement si elle ne perturbe pas son activité et ses opérations, ni l'exercice des fonctions des autres utilisateurs. L'utilisation du réseau Wi-Fi de l'entreprise à des fins de loisirs est également soumise à cette condition.

Il est interdit de connecter des commutateurs réseau, des distributeurs, des points d'accès sans fil et des routeurs à des périphériques réseau actifs au réseau de l'entreprise. Toutes les adresses IP seront attribuées et gérées exclusivement par l'entreprise ;

11.7. Les employés ne peuvent quitter l'entreprise qu'avec une autorisation écrite préalable et explicite. L'accès aux services informatiques de la Société par des personnes extérieures, etc., est interdit ; 11.8. Tout utilisateur des ressources informatiques de la Société est tenu de respecter la Politique de sécurité de l'information de la Société, y compris les CONDITIONS D'UTILISATION DES RESSOURCES INFORMATIQUES et toutes les dispositions légales et autres, réglementations, règles et usages applicables. En particulier, et sans que cette liste soit exhaustive, tout utilisateur est tenu d'agir conformément aux clauses suivantes :

11.8.1. Ne divulguez à personne le mot de passe et le nom d'utilisateur qui vous ont été attribués par la société.

11.8.2. L'accès aux ressources informatiques ne sera pas autorisé, que ce soit à l'intérieur ou à l'extérieur de l'entreprise, sauf à des fins autorisées, et l'accès à ces ressources ne sera pas facilité à des fins non autorisées par d'autres personnes ;

11.8.3. Aucun matériel ni ressource ne peut être utilisé ou introduit dans le réseau qui permettrait un accès, une modification ou une perturbation non autorisés de toute ressource informatique, comme le scan de ports, au sein de l'entreprise ou ailleurs ; 11.8.4. Tout ce qui pourrait être considéré comme offensant ou préjudiciable à la réputation de l'entreprise.

Les images ou textes contenant des éléments pornographiques, pédophiles, sexistes, racistes, diffamatoires, menaçants, injurieux, illégaux, discriminatoires ou liés au terrorisme, susceptibles de nuire à autrui, ne peuvent être affichés, stockés, reçus ou transmis dans les systèmes et les fichiers ; 11.8.5. Les signatures et/ou en-têtes de courrier électronique ne peuvent être usurpés, les courriels en chaîne, indésirables ou de harcèlement ne peuvent être créés et/ou transmis, l'usurpation d'identité ne peut être utilisée pour agir au nom d'autrui dans les communications électroniques, et les communications inutiles ou offensantes ne peuvent être créées ;

11.8.6. Tous les appareils mobiles utilisés pour accéder aux ressources fournies par la société dans le cadre de ses services informatiques doivent être cryptés à l'aide d'un logiciel de cryptage approprié et protégés par un code PIN ou un mot de passe ;

11.8.7. Tous les matériels et logiciels fournis par la société et des tiers

Les droits d'auteur seront respectés et les documents protégés par le droit d'auteur, y compris les logiciels et les données acquises, ne seront ni utilisés, ni téléchargés, ni copiés, ni stockés sur le système, ni fournis, sauf avec l'autorisation du titulaire des droits d'auteur ou conformément aux termes de la licence détenue par la Société ; 11.8.8. Lors du traitement des données concernant des personnes physiques, les dispositions de la législation sur la protection des données seront respectées.

La politique de protection des données de l'entreprise sera appliquée pour traiter (collecter, utiliser, partager et détruire) les données de manière appropriée. 11.8.9. Données générées/détenues/ appartenant à l'utilisateur sur les ressources informatiques de l'entreprise

Il convient de noter que toutes les données stockées peuvent faire l'objet d'un audit par la Société ou les autorités compétentes en cas de suspicion d'infractions. Si les données concernées sont chiffrées, l'utilisateur est tenu de fournir la clé de déchiffrement ; 11.8.10. Les conditions de licence de tous les logiciels et contenus utilisés via une plateforme quelconque doivent être définies et respectées ; 11.9. Conformément à l'article 6 de la loi n° 5561 relative à la réglementation des publications sur Internet et à la lutte contre la criminalité en ligne, la Société prend les mesures nécessaires pour stocker les informations relatives au trafic de communications électroniques reçues ou envoyées par elle, dans la limite des finalités prévues par la loi, et pour garantir l'exactitude, l'intégrité et la confidentialité de ces informations. Les modalités de mise en œuvre de ces mesures sont régies par les Principes d'application relatifs aux communications électroniques et à l'audit des données.

En cas d'incident de sécurité des données survenu ou suspecté (article 11.10), le responsable du département informatique peut prendre rapidement des mesures pour résoudre l'incident ou atténuer les dommages potentiels, comme le blocage de l'accès des utilisateurs au système ou l'inspection des appareils connectés au réseau.

11.11. Si une enquête plus approfondie est jugée nécessaire, le service informatique contactera l'entreprise. Avec l'autorisation expresse du Conseil d'administration, la Société peut prendre les mesures nécessaires pour examiner tout système sur son réseau. 11.12. Sauf disposition contraire de la loi applicable, la Société ne saurait être tenue responsable de toute perte, dommage ou événement indésirable découlant directement ou indirectement de l'utilisation ou de l'empêchement de l'utilisation des ressources informatiques fournies et/ou gérées par elle.

11.13. Bien que la Société ne soit pas responsable de l'accès non autorisé ou de la modification des données personnelles et autres. Bien que le fournisseur prenne des mesures de sécurité appropriées contre la divulgation, la destruction ou la perte accidentelle des données, il ne donne aucune garantie à l'utilisateur quant à la sécurité, la confidentialité ou l'intégrité des données. 11.14.

Le nom, l'adresse, la photographie, l'état civil, l'adresse électronique, le nom d'utilisateur, le pseudonyme, la carte d'identité de l'entreprise et autres informations pertinentes des utilisateurs seront stockés sur des supports informatiques pour être utilisés à d'autres fins telles que l'administration et le suivi de l'utilisation du système.

11h15. Les conditions mentionnées ci-dessus s'appliquent également aux utilisations du réseau de la Société par des appareils n'appartenant pas à la Société, tels que les ordinateurs portables personnels et les ordinateurs domestiques, lorsqu'ils se connectent au réseau de la Société directement et/ou via un VPN. 11.16. Le non-respect des conditions susmentionnées peut entraîner des mesures disciplinaires, notamment la suspension de l'accès à toutes les ressources informatiques de l'entreprise pour des périodes déterminées et/ou l'imposition de sanctions. En cas de manquements graves, l'entreprise se réserve le droit de résilier le contrat de travail de la personne concernée et d'engager des poursuites civiles et pénales à son encontre. Les employés de l'entreprise agissent en qualité de mandataires pour les invités utilisant les infrastructures informatiques et/ou la connexion internet fournies par l'entreprise. Ces employés sont responsables des actions de leurs invités et doivent en assurer le suivi.