أمن المعلومات و
سياسة إطار البيانات الشخصية

رقم الوثيقة	IKVKK_P1الإصدار 1.00
تاريخ المراجعة	-
تاريخ النشر	27/05/2024
صفحة	13

شركة كارديلين المحدودة لتجارة صناعة الدهانات والمواد الكيميائية

إطار أمن المعلومات والبيانات الشخصية
سياسة

1.المقدمة والغرض

1.1.تم إعداد هذه الوثيقة لتحديد سياسة إطار أمن المعلومات والبيانات الشخصية لشركة Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi(المشار إليها فيما يلي باسم سياسة الإطار)، والتي ترد تفاصيلها أدناه.

شركة Kardelenلتجارة الطلاء والصناعة الكيماوية المحدودة: Alcı OSB Mah. 2036كاد. رقم: 7
سينجان/أنقرة، تركيا
+90 312 398 11 33
kvkk@kardelenboya.com.tr
http://www.kardelenboya.com.tr/إنتاج الدهانات:

مراقب البيانات	
عنوان	
الهاتف	
بريد	
موقع إلكتروني	
مجال النشاط	

توفر سياسة الإطار هذه نظرة عامة على سياسات الشركة ولوائحها وبيانات الإفصاح والإرشادات المعمول بها فيما يتعلق بأمن المعلومات وخصوصية البيانات الشخصية، وتهدف أيضًا إلى إظهار التزام الشركة بالتدريب ورفع مستوى الوعي في هذه المجالات.

١.٢.تهدف هذه السياسة الإطارية إلى توفير الشروط اللازمة والصالحة للمعالجة القانونية والآمنة والفعالة والكفؤة لجميع المعلومات والبيانات التي تحصل عليها شركتنا. تُعدّ معالجة المعلومات والبيانات أمرًا حيويًا لتسيير وإدارة عمليات شركتنا اليومية. وتعتمد جودة الخدمات التي تقدمها الشركة، وتخطيطها، وقياس أدائها، وسلامتها المهنية، وتأمينها، وإدارتها المالية، اعتمادًا كبيرًا على عمليات جمع المعلومات ومعالجتها بدقة وموثوقية. تتطلب حوكمة المعلومات السليمة والموثوقة إدارةً ومساءلةً فعّالة وشفافة، وعمليات حوكمة، وسياسات وإجراءات موثقة، وموظفين مدربين، وموارد كافية. وبناءً على ذلك، ستحدد هذه السياسة الإطارية الشروط والمعايير وأفضل الممارسات السارية في مجال إدارة موارد المعلومات والمعالجة القانونية للبيانات الشخصية.

1.3.يُعدّ أمن المعلومات وحماية البيانات الشخصية مسؤوليةً أساسيةً تقع على عاتق كل موظف في شركتنا. ويتحمّل كل موظف مسؤولية تطبيق ممارسات العمل في الشركة واستيعاب سياساتها وقواعد العمل الخاصة بها.

لذا، من الضروري أن يكون كل موظف لدينا على دراية بالمسائل الواردة في هذه الوثيقة الإطارية. كما يُتوقع من الأطراف الثالثة التي تستخدم بيانات الشركة الالتزام بالمبادئ المنصوص عليها في هذه الوثيقة الإطارية.

.1.4الغرض من سياسة الإطار هذه هو مساعدة شركتنا في الوفاء بالمسؤوليات التالية:

•الامتثال للالتزامات القانونية والإدارية والتعاقدية؛
•ضمان الحوكمة الرشيدة للشركات؛ •تقديم خدمات عالية الجودة؛ •حماية الموارد المالية للشركة؛ •تخطيط عمليات استمرارية الأعمال المناسبة؛ •ضمان استمرار أمن معاملات البيانات الخاضعة لسيطرة الشركة.

التوفير والتطوير.

.1.5تقوم الشركة يومياً بتنفيذ مجموعة واسعة من أنشطة جمع ومعالجة البيانات الشخصية القياسية والمتخصصة اللازمة لتقديم الخدمات، وضمان استمرارية العلاقات والالتزامات التجارية، وضمان الأمن الوظيفي لموظفيها.

.2النطاق

.2.1تنطبق سياسة الإطار هذه على جميع البيانات التي تحتفظ بها شركتنا والتي تتم معالجتها من قبل الأطراف التي تعالج البيانات نيابة عن الشركة، بما في ذلك البيانات المدرجة أدناه على سبيل المثال، سواء كانت في شكل إلكتروني أو مادي:

•يتم تخزينها بواسطة أجهزة الكمبيوتر المكتبية أو المحمولة وأجهزة التخزين
•معالجة البيانات الإلكترونية؛ •نقل البيانات عبر الشبكات؛

•المعلومات المرسلة باستخدام الفاكس وطرق نقل البيانات المماثلة؛ •السجلات المحفوظة في جميع أنواع الوسائط الورقية؛ • المواد المرئية والفوتوغرافية، بما في ذلك الميكروفيش والشرائح وتسجيلات نظام الكاميرا ذات الدائرة المغلقة؛

•بيانات الاتصال اللفظي، بما في ذلك الاتصال وجهاً لوجه والرسائل الصوتية والمحادثات المسجلة.

.2.2يجب على الأطراف المدرجة أدناه الامتثال للإجراءات والمبادئ المنصوص عليها في هذه الوثيقة الإطارية.
من الضروري القيام بما يلي:

•جميع موظفي الشركة؛
•جميع الأطراف الثالثة المصرح لها بالوصول إلى بيانات الشركة، بما في ذلك المستشارين ومقدمي الخدمات والمقاولين والزوار.

.2.3تتألف سياسة الإطار هذه من جزأين. يصف الجزء الأول استراتيجية شركتنا فيما يتعلق بأمن المعلومات وحماية البيانات الشخصية، بينما يصف الجزء الثاني...

يصف هذا القسم أدوار ومسؤوليات أصحاب المصلحة المعنيين في هذا الصدد، بالإضافة إلى السياسات وبرامج التدريب التي سيتم تنفيذها في هذا المجال.

.2.4فيما يلي معلومات حول كيفية تصنيف البيانات الخاضعة لسيطرة الشركة.

يتم توفير ما يلي:

(1)تُعرَّف "البيانات الشخصية" بأنها أي معلومات تتعلق بشخص طبيعي مُحدَّد أو قابل للتحديد ("صاحب البيانات")؛ والشخص الطبيعي المُحدَّد هو الشخص الذي يمكن تحديده بشكل مباشر أو غير مباشر بالرجوع إلى اسمه، أو رقم هويته، أو بيانات موقعه، أو مُعرِّفه الإلكتروني، أو عامل واحد أو أكثر من العوامل الخاصة بهويته الجسدية، أو الفسيولوجية، أو الجينية، أو العقلية، أو الاقتصادية، أو الثقافية، أو الاجتماعية. ويجب الالتزام بالإجراءات والمبادئ المنصوص عليها في سياسة الشركة لمعالجة البيانات الشخصية وحمايتها عند جمع البيانات الشخصية واستخدامها وتخزينها.

(2)تُعدّ البيانات المتعلقة بعرق الشخص، أو أصله الإثني، أو رأيه السياسي، أو معتقداته الفلسفية، أو دينه، أو طائفته، أو معتقداته الأخرى، أو مظهره وملابسه، أو عضويته في الجمعيات أو المؤسسات أو النقابات العمالية، أو صحته، أو حياته الجنسية، أو سجله الجنائي، أو تدابيره الأمنية، بالإضافة إلى البيانات البيومترية والوراثية، فئات خاصة من البيانات الشخصية. وتُحدد الشروط الإضافية والتدابير الوقائية لتعزيز أمن معالجة هذه الفئات الخاصة من البيانات الشخصية في سياسات الشركة الخاصة بمعالجة البيانات الشخصية وحمايتها وأمن البيانات.

(3)البيانات التالية، باستثناء البيانات الشخصية، هي بيانات خاصة بالشركة:
سيُشار إليها باسم البيانات:

(أ) بيانات التخطيط/الإدارة أو البحث، والمعلومات المحمية قانونًا بموجب اتفاقيات وبنود السرية، وما إلى ذلك، والتي تتمتع بحماية تجارية.

بيانات الشركات الحساسة. يجب حماية هذه البيانات باستخدام أحدث التدابير الأمنية؛

(ب) البيانات غير الخاصة المتعلقة بالشركة والتي لم يتم الكشف عنها علنًا والتي يجوز الكشف عنها بموجب المتطلبات القانونية مثل قانون حرية المعلومات.

.3الهدف

.3.1تهدف استراتيجية شركتنا إلى ضمان ثقة عملائنا وشركائنا وموردينا في معالجة البيانات وتخزينها بما يتناسب مع قيمتها ومخاطرها، وضمان وفاء شركتنا بمسؤولياتها القانونية في مجالات إدارة المعلومات وأمنها وحماية البيانات الشخصية. ينبغي على جميع الأطراف المعنية إدراك أهمية الاستخدام السليم للبيانات، وجمعها ومعالجتها بشكل قانوني، وحمايتها من سوء الاستخدام.

.3.2يهدف هذا النهج إلى ضمان التزام شركتنا بالمسؤوليات القانونية والأخلاقية المطبقة على المجالات التالية:

•المعالجة القانونية للبيانات المتعلقة بالأشخاص المحددين أو القابلين للتحديد
استخدامها وحماية سلامتها؛
•يجب الوصول إلى البيانات فقط وفقًا للقانون.
•نقل البيانات الشخصية إلى الأفراد؛ •وضع إطار تنظيمي ينطبق على إدارة المعلومات؛ •أحكام لتسجيل البيانات الشخصية ومشاركتها واستخدامها.

مدونة قواعد السلوك المتعلقة بالحصول على موافقة صريحة؛

•مدونة قواعد السلوك والممارسات المهنية التي تقبلها الشركة
وتشمل التوجيهات ما يلي: •تبادل المعلومات والبيانات مع أطراف ثالثة.

3.3. تهدف الاستراتيجية إلى الحفاظ على معايير أمنية مناسبة في مجال إدارة المعلومات، بالإضافة إلى المعايير العالية المتوقعة من هوية الشركة، وإلى ترسيخ ثقافة أمن البيانات الشخصية بشكل كامل في جميع أنحاء الشركة.

3.4. فيما يلي الأهداف الاستراتيجية للشركة فيما يتعلق بأمن المعلومات وخصوصية البيانات الشخصية:

•ينبغي أن تدعم إدارة المعلومات الاستراتيجية العامة للشركة واستراتيجياتها الفرعية وبرامج التحول المؤسسي ذات الصلة، كما ينبغي أن تلعب ممارسات أمن المعلومات دورًا أساسيًا في تطوير هذه الاستراتيجيات والبرامج وتنفيذها. •يجب إنشاء البنية التحتية والعمليات اللازمة لضمان وصول المعلومات الصحيحة إلى الشخص المناسب في الوقت المناسب وللغرض المناسب، كما يجب تحديد البنية التحتية والعمليات اللازمة لضمان تسليم هذه المعلومات بطريقة أخلاقية وقانونية وفعالة ومناسبة.

•تطوير حلول مبتكرة في إدارة المعلومات، مع مراعاة تحول عمليات الأعمال؛ •دمج إدارة المعلومات في العمليات الإدارية للشركة من خلال تنفيذ تغييرات سلوكية شاملة للاعتراف بالمعلومات كأصل أساسي؛

•جوانب محددة لإدارة المعلومات تتعلق بمؤهلات الموظفين والأوصاف الوظيفية.
تحديد الشروط؛
•تشجيع الموظفين على العمل معًا لمنع بذل جهد غير ضروري وضمان استخدام أكثر كفاءة للموارد؛ •العمل على ضمان وجود المعايير المعمول بها للامتثال للالتزامات والسياسات القانونية والإدارية والتعاقدية؛

•تحديد وإدارة موارد المعلومات داخل الشركة وإنشاء نظام لإدارة مخاطر المعلومات يوازن بين المخاطر والفرص التي تنطبق على موارد المعلومات هذه؛

•ضمان ثقة جميع الأطراف المعنية من خلال تنفيذ التدابير اللازمة والمتناسبة لتطبيق أفضل معايير الممارسات لحماية موارد المعلومات؛

•توفير التدريب الكافي لجميع موظفينا وشركائنا الرئيسيين، ورفع مستويات الوعي، وضمان فهم جميع البيانات والمعلومات التي تتم معالجتها داخل الشركة بشكل صحيح.

تهيئة بيئة ثقافية مناسبة لمعالجة القضايا بشعور من المسؤولية والواجب.

.4نهج شركتنا

.4.1يتم دمج أمن المعلومات وحماية البيانات الشخصية بشكل كامل في أنشطة شركتنا. وفي هذا الصدد، نأخذ في الاعتبار أربعة عناصر رئيسية لعمليات الشركة:

•العنصر البشري
•العمليات
•المعلومات •التكنولوجيا

.4.2في أنشطة إدارة المعلومات وتطويرها وحمايتها، يتم تقييم العوامل المذكورة أعلاه من حيث كيفية مساهمتها في تحقيق أهدافنا الاستراتيجية.

.4.3من المخطط أن تتحقق أهدافنا الاستراتيجية في مجال إدارة المعلومات من خلال السياسات التي سيتم وضعها. عند تطوير برامج وعمليات مؤسسية جديدة، سيتم تحديد كل مشروع لإدارة المعلومات وتنفيذه ومراقبته وفقًا للنهج واللوائح الإدارية الموضحة في هذه السياسة الإطارية.

.4.4من المتوقع أن يؤدي تطبيق الاستراتيجية المذكورة أعلاه إلى تحقيق الفوائد التالية:

•تتم معالجة المعلومات والبيانات داخل الشركة بطريقة متسقة وفعالة.
إدارة؛
•فهم أفضل للتشريعات ذات الصلة ومستوى الامتثال لأحكامها
متزايد؛
•الأحداث التي تؤثر على أمن المعلومات وخصوصية البيانات الشخصية
مما يقلل بشكل كبير من تكراره؛
•الوقت والجهد الذي يتعين على الموظفين بذله في هذا الشأن
•تقليل؛ •تحسين جودة البيانات؛ •تحديد المسؤوليات التي يجب القيام بها فيما يتعلق بإدارة المعلومات والأمن
بشكل واضح.

ليتم تقديمها بطريقة ما؛
•إدارة المخاطر التي تهدد أمن المعلومات والبيانات بشكل فعال؛

.4.5يتولى المدير العام للشركة مسؤولية تنفيذ هذه الاستراتيجية. وتتولى لجنة حماية البيانات الشخصية، برئاسة المدير العام، مسؤولية مراقبة هذه السياسة الإطارية والسياسات والتوجيهات ذات الصلة على مدار العام، وتقديم تقارير عن التقدم المحرز. وسيتم تنفيذ استراتيجية أمن المعلومات وحماية البيانات الشخصية من خلال سياسات وبرامج تطوير ومشاريع متفق عليها. وفي نهاية كل عام، ستقوم لجنة حماية البيانات الشخصية بمراجعة الاستراتيجية.

بناءً على الأولويات المتفق عليها والموارد المتاحة، سيوافق المدير العام على برامج التطوير المخطط لها للعام التالي. كما سيُقرّ المدير العام برامج التطوير التي وافقت عليها لجنة حماية البيانات الشخصية.

4.6.التعاريف

4.6.1نظام إدارة أمن المعلومات .(ISMS)

4.6.2المخزون: جميع أصول المعلومات المهمة للشركة.

4.6.3الإدارة العليا: يشير هذا إلى الإدارة العليا للشركة.

4.6.4المعرفة العملية: القدرة على فعل شيء ما.

4.6.5المعلومات السرية: تُعدّ المعلومات، شأنها شأن جميع أصول الشركات والأعمال الأخرى، أصولاً ذات قيمة للشركة، وبالتالي يجب حمايتها بشكل مناسب. داخل الشركة، تُعتبر المعرفة الفنية، والعمليات، والصيغ، والتقنيات، والأساليب، وسجلات العملاء، ومعلومات التسويق والمبيعات، ومعلومات الموظفين، والمعلومات التجارية والصناعية والتكنولوجية، والأسرار، معلومات سرية.

4.6.6الخصوصية: تشير هذه النقطة إلى تقييد الوصول إلى محتوى المعلومات بحيث يقتصر على الأشخاص المصرح لهم فقط بالاطلاع عليها/على البيانات. (مثال: إرسال البريد الإلكتروني المشفر يمنع الأشخاص غير المصرح لهم من قراءة رسائل البريد الإلكتروني حتى في حال اعتراضها -البريد الإلكتروني المسجل (KEP -

4.6.7سلامة البيانات: تشير هذه النقطة إلى ضمان إمكانية اكتشاف أي تعديلات أو حذف أو إضافة غير مصرح بها أو عرضية على المعلومات، وضمان إمكانية تتبعها. (مثال: تخزين البيانات في قاعدة البيانات مع معلومات موجزة -التوقيع الإلكتروني -التوقيع عبر الهاتف المحمول)

4.6.8التوافر/التوفر: يشير هذا إلى جاهزية الأصل للاستخدام عند الحاجة. بعبارة أخرى، يجب أن تكون الأنظمة متاحة باستمرار، ويجب عدم فقدان البيانات الموجودة عليها، ويجب أن تكون قابلة للوصول إليها بشكل دائم. (مثال: استخدام وحدات تزويد الطاقة غير المنقطعة ووحدات تزويد الطاقة الاحتياطية في هياكل الخوادم لحمايتها من تقلبات خطوط الطاقة وانقطاع التيار الكهربائي .(UPS -

4.6.9أصول المعلومات: هي أصول مملوكة للشركة ضرورية لاستمرار عملياتها دون انقطاع. وفي نطاق العمليات التي تغطيها هذه السياسة، تشمل أصول المعلومات ما يلي:

•جميع أنواع المعلومات المقدمة في الوسائط الورقية أو الإلكترونية أو المرئية أو السمعية، و
بيانات،

•أي برنامج يُستخدم للوصول إلى المعلومات وتعديلها، و
الأجهزة،

•الشبكات التي تُمكّن من نقل المعلومات،

•المرافق والمناطق الخاصة،

•الإدارات والوحدات والفرق والموظفين،

•شركاء الحلول،

•هذه خدمات أو منتجات أو عروض مقدمة من أطراف ثالثة.

4.7.يحدد المخطط التنظيمي المضمن في الملحق الخاص بهذه السياسة الإطارية الجهات الفاعلة وأدوارها في إدارة المعلومات داخل الشركة.

4.7.1مسؤولية الإدارة

- تلتزم إدارة الشركة بالامتثال لنظام أمن المعلومات وحماية البيانات الشخصية المُحدد والمُطبق والقابل للتنفيذ، وتخصيص الموارد اللازمة لتشغيل النظام بكفاءة، وضمان فهم جميع الموظفين له. يتحمل المدير العام المسؤولية العامة عن ضمان تقييم مخاطر أمن المعلومات والتخفيف من آثارها، وسيضمن نشر السياسات والتوعية ذات الصلة لجميع المعنيين داخل الشركة. ستُعامل مخاطر أمن المعلومات والبيانات على قدم المساواة مع عوامل المخاطر المالية والقانونية ومخاطر سمعة الشركة الأخرى.

- أثناء إعداد نظام أمن المعلومات وحماية البيانات الشخصية، يتم تعيين مسؤول اتصال البيانات بموجب وثيقة تكليف مكتوبة. وإذا لزم الأمر، يجوز للإدارة العليا مراجعة الوثيقة وإعادة التعيين.

- يُساعد المديرون في المستويات الإدارية العليا الموظفين في المستويات الأدنى من خلال تحديد المسؤوليات وتقديم القدوة الحسنة فيما يتعلق بالأمن. هذا النهج، الذي يبدأ من أعلى المستويات ويُطبّق وصولاً إلى أدنى الموظفين، أمرٌ بالغ الأهمية.

لذلك، يشجع جميع المديرين موظفيهم، كتابياً وشفهياً، على اتباع تعليمات السلامة والمشاركة في الأنشطة المتعلقة بالسلامة.

-خصصت الإدارة العليا الميزانية اللازمة لجهود أمن المعلومات الشاملة.
إنه يخلق.
يكون مسؤول الاتصال بالبيانات مسؤولاً أمام الإدارة العليا المعينة عن توقيع اتفاقيات مشاركة البيانات ومعالجتها والبروتوكولات التكميلية مع أصحاب المصلحة المعنيين، بالإضافة إلى إعداد الاتفاقيات والبروتوكولات الأخرى المطبقة على الوصول إلى البيانات ونقلها المطلوبة في نطاق عمليات الشركة.

4.7.2.جهة الاتصال بالبيانات

يتولى مسؤول الاتصال بالبيانات مسؤولية إعداد وتنفيذ الرؤية والاستراتيجيات والبرامج المؤسسية اللازمة لحماية أصول وأنظمة المعلومات الخاصة بالشركة. وفيما يلي قائمة بمهامه في هذا الشأن:

- يُعدّ تخطيط نظام أمن المعلومات وحماية البيانات الشخصية مقبولاً.
  تحديد مستوى المخاطر، وتحديد منهجية تقييم المخاطر،

- توفير الموارد اللازمة لدعم الأنشطة التكميلية في إنشاء نظام أمن المعلومات وحماية البيانات الشخصية، وضمان/تحسين قدرات المستخدمين ورفع مستوى الوعي، وإجراء التدريب، وضمان التواصل، وتوفير متطلبات التوثيق.

- تنفيذ وإدارة تطبيقات نظام أمن المعلومات وحماية البيانات الشخصية، وضمان استمرارية عمليات التقييم والتحسين وتقييم المخاطر.

- عمليات التدقيق الداخلي، واجتماعات مراجعة الأهداف والإدارة، وأمن المعلومات
  وتقييم نظام وضوابط حماية البيانات الشخصية،

- الحفاظ على الهيكل الحالي وضمان التحسينات المستمرة في نظام أمن المعلومات وحماية البيانات الشخصية.

4.7.3رؤساء الأقسام

- إجراء دراسات جرد الأصول وتحليل المخاطر المتعلقة بالأقسام،

- يُطلب من مسؤول الاتصال بالبيانات إجراء تقييم للمخاطر كلما حدث تغيير في أصول المعلومات التي تقع تحت مسؤوليته والتي قد تؤثر على مخاطر أمن المعلومات.
  معلومة،

- يجب على الموظفين الخاضعين لإشرافه/إشرافها الالتزام بسياسات الشركة ولوائحها.
  ضمان تشغيلها وفقًا للإجراءات،

- رفع مستوى الوعي وضمان التواصل في نطاق نظام إدارة أمن المعلومات فيما يتعلق بالإدارات،
  توفير متطلبات التوثيق،

- في نظام إدارة أمن المعلومات، يتمثل الهدف في الحفاظ على الهيكل الحالي وضمان التحسينات المستمرة.
  هو المسؤول.

- يتحمل رؤساء الأقسام مسؤولية تقييم جوانب إدارة المعلومات ضمن إجراءات العمل في أقسامهم وفي الأنشطة التي تُنفذ بالتعاون مع الجهات المعنية. يُرجى مراجعة سياسة أمن المعلومات للاطلاع على المسؤوليات المحددة المتعلقة بأمن المعلومات.

4.7.4مسؤولية جميع الموظفين

- إنهم مسؤولون عن القيام بعملهم وفقًا لأهداف وسياسات أمن المعلومات ووثائق نظام إدارة أمن المعلومات.

- مراقبة أهداف أمن المعلومات المتعلقة بالوحدة الخاصة والمساهمة في تحقيق هذه الأهداف.

- أي مشكلات تتعلق بأمن المعلومات يتم ملاحظتها أو الاشتباه بها في الأنظمة أو الخدمات.
من خلال الانتباه إلى أي ثغرات أو انتهاكات والإبلاغ عنها،

- بالإضافة إلى اتفاقيات الخدمة (الاستشارات، وما إلى ذلك) مع أطراف ثالثة والتي لا تقع مسؤوليتها على عاتق المشتري، فإنه مسؤول عن وضع اتفاقيات السرية وضمان متطلبات أمن المعلومات.

- يجب على جميع موظفي الشركة والجهات الخارجية المصرح لها بالوصول إلى أصول معلومات الشركة الالتزام بالقوانين واللوائح، مع إدراك مسؤولياتهم الشخصية في إدارة المعلومات. كما يجب على جميع الموظفين الالتزام بسياسات الشركة وإجراءاتها وتوجيهاتها المعتمدة، والمشاركة في الدورات التدريبية والفعاليات المتعلقة بإدارة المعلومات.

.5المبادئ العامة لأمن المعلومات

.5.1يلتزم موظفو الشركة والأطراف الثالثة بالإلمام بالتفاصيل والإجراءات المتعلقة بمتطلبات وقواعد أمن المعلومات المنصوص عليها في سياسة الإطار هذه، والقيام بعملهم وفقًا لهذه القواعد.

.5.2ما لم ينص على خلاف ذلك، يجب مراعاة هذه القواعد والسياسات لجميع المعلومات المخزنة والمعالجة في شكل مطبوع أو إلكتروني، ولاستخدام جميع أنظمة المعلومات.

.5.3يتم هيكلة نظام أمن المعلومات وحماية البيانات الشخصية وتشغيله بناءً على قانون حماية البيانات الشخصية التركي (KVKK) واللائحة العامة لحماية البيانات (GDPR)ومعيار TS ISO/IEC 27001"تقنيات أمن تكنولوجيا المعلومات ومتطلبات أنظمة إدارة أمن المعلومات".

.5.4يتم تنفيذ نظام أمن المعلومات وحماية البيانات الشخصية وتشغيله وتحسينه بمساهمة الأطراف المعنية. ويتولى مسؤول الاتصال بالبيانات مسؤولية تحديث الوثائق ذات الصلة عند الضرورة.

إنها مسؤوليتهم.

.5.5ما لم ينص القانون أو العقد على خلاف ذلك، فإن أنظمة المعلومات والبنية التحتية التي توفرها الشركة للموظفين أو الأطراف الثالثة، وجميع المعلومات والوثائق والمنتجات التي يتم إنتاجها باستخدام هذه الأنظمة، مملوكة لشركة .Kimya Sanayi Ticaret Limited Şirketi Kardelen Boya ve

.5.6يتم توقيع اتفاقيات السرية مع الموظفين والمستشارين ومقدمي الخدمات (الأمن والنقل والتموين وشركات التنظيف وما إلى ذلك) والموردين والمتدربين.

.5.7المعلومات التي سيتم تطبيقها في عمليات التوظيف وتغيير الوظائف وإنهاء الخدمة.
يتم تحديد وتنفيذ الضوابط الأمنية.

.5.8يتم تقديم دورات تدريبية بانتظام للموظفين الحاليين والجدد لزيادة وعي الموظفين بأمن المعلومات وتمكينهم من المساهمة في تشغيل النظام.

.5.9يتم الإبلاغ عن جميع حالات الاختراق الفعلية أو المشتبه بها لأمن المعلومات؛ ويتم تحديد المخالفات التي تسببت في هذه الاختراقات، وتحديد أسبابها الجذرية، واتخاذ التدابير اللازمة لمنع تكرارها.

5.10.يتم إنشاء قائمة بأصول المعلومات وتحديد ملكية الأصول وفقًا لاحتياجات إدارة أمن المعلومات.

5.11.يتم تصنيف البيانات الشخصية وبيانات الشركات، ويتم ضمان أمن البيانات في كل فئة.
يتم تحديد الاحتياجات وقواعد الاستخدام.

5.12.الأمن المادي بما يتماشى مع احتياجات الأصول المخزنة في المناطق الآمنة.
يتم تطبيق الضوابط.

5.13.انكشاف أصول المعلومات الخاصة بالشركة داخل المنظمة وخارجها.
يتم وضع وتنفيذ الضوابط والسياسات اللازمة لمواجهة التهديدات المادية.

5.14.يتم تطوير وتنفيذ الإجراءات والتعليمات المتعلقة بإدارة السعة، والعلاقات مع الأطراف الثالثة، والنسخ الاحتياطي، وقبول النظام، وعمليات الأمان الأخرى.

5.15.يتم تعديل تكوينات إنشاء سجلات التدقيق لأجهزة الشبكة وأنظمة التشغيل والخوادم والتطبيقات وفقًا لاحتياجات الأمان الخاصة بالأنظمة المعنية.
تتم حماية سجلات التدقيق من الوصول غير المصرح به.

5.16.تُمنح صلاحيات الوصول حسب الحاجة. وتُستخدم أكثر التقنيات والأساليب أمانًا المتاحة للتحكم في الوصول.

5.17.يتم تحديد متطلبات الأمن في عملية شراء وتطوير النظام.
أثناء عملية القبول أو الاختبار، يتم التحقق مما إذا كانت متطلبات السلامة مستوفاة.

5.18.يتم إعداد خطط استمرارية العمل وصيانتها وممارستها للبنية التحتية الحيوية.

5.19.تم تصميم العمليات لضمان الامتثال للقوانين والسياسات والإجراءات المحلية ومعايير السلامة الفنية؛ ويتم ضمان الامتثال من خلال أنشطة المراقبة والتدقيق المستمرة والدورية.

6.السياسات التي سيتم وضعها في نطاق سياسة إطار أمن المعلومات والبيانات الشخصية

6.1.فيما يلي اللوائح التي تحدد السياسات وقواعد السلوك المتوقع وضعها في نطاق سياسة إطار أمن المعلومات والبيانات الشخصية:

عنوان	مرجع نوع المستند رقم	
أمن المعلومات والشخصية سياسة إطار البيانات	KVKK_P1	سياسة
حماية البيانات الشخصية وسياسة معالجتها	KVKK_P2	سياسة
سياسة تخزين البيانات الشخصية وإتلافها	KVKK_P3	سياسة

المعلومات الشخصية التي تنطبق على الموظفين بيانات سياسة	KVKK_P4	سياسة
سياسة أمن المعلومات	KVKK_P5	سياسة
المعلومات والاتصالات استخدام التقنيات سياسة	KVKK_P6	سياسة
سياسة التحكم في الوصول	KVKK_P7	سياسة
أنظمة كاميرات داخلية سياسة	KVKK_P8	سياسة
قبول الإنترنت وأدوات الاتصال الإلكترونية يمكن القيام بذلك الإجراءات والمبادئ المتعلقة بـ السياسات ذات الصلة	KVKK_P9	سياسة
سياسة كاميرات المركبات	KVKK_P10	سياسة
موضوعات البيانات استخدام تطبيقاتهم مبادئ وإجراءات الإجابات اللوائح المتعلقة بـ	KVKK_Y1	أنظمة
خطة الاستجابة لاختراق البيانات أنظمة	KVKK_Y2	أنظمة
تأثير حماية البيانات إجراءات التقييم و حول مبادئها أنظمة	KVKK_Y3	أنظمة
الاتصالات الإلكترونية و البيانات الإلكترونية حول عملية التفتيش أنظمة	KVKK_Y4	أنظمة
الرسائل الإلكترونية إجراءات الاستخدام و اللوائح المتعلقة بمبادئها	KVKK_Y5	أنظمة
كاميرا الدائرة المغلقة إجراءات استخدام الأنظمة وعن مبادئها أنظمة	KVKK_Y6	أنظمة
كلمات مرور المستخدم التعريف والاستخدام و إجراءات تتعلق بحمايتها حول المبادئ أنظمة	KVKK_Y7	أنظمة
إجراءات أمن نقل البيانات وعن مبادئها أنظمة	KVKK_Y8	أنظمة
صالحة للتقديم على الوظائف. نص معلومات اللائحة العامة لحماية البيانات	نص حماية البيانات KVKK_A1	
إنترنت الاستخدام نص معلوماتي	نص حماية البيانات KVKK_A2	

أنظمة كاميرات داخلية نص معلوماتي	نص حماية البيانات KVKK_A3	
نص معلومات قانون حماية البيانات الشخصية (KVKK)	نص حماية البيانات KVKK_A4	
إضاءة الموقع الإلكتروني نص	نص حماية البيانات KVKK_A5	
حماية البيانات الشخصية نبذة عن المقاول نص معلوماتي	نص حماية البيانات KVKK_A6	
نص معلومات الزائر	نص حماية البيانات KVKK_A7	
تأثير حماية البيانات نموذج التقييم	KVKK_F1	
البيانات الشخصية ملحق بشأن حمايته بروتوكول	KVKK_S1	اتفاق

6.2.صنع السياسات

6.2.1.تقوم لجنة البيانات الشخصية بمراجعة جميع سياسات إدارة أمن المعلومات، وإذا رأت ذلك ضرورياً، ترفع توصياتها بشأن التغييرات إلى الإدارة العليا. ويتم إبلاغ الموظفين بجميع السياسات المعمول بها والتحديثات ذات الصلة عبر بوابة الشركة أو الإنترنت.

6.2.2.تُراجع السياسات سنوياً وتُحدّث حسب الحاجة، وقد تُوضع سياسات جديدة لمعالجة أوجه القصور. وعند الاقتضاء، تُؤخذ هذه السياسات بعين الاعتبار بالتزامن مع عقد عمل الموظف.

6.2.3.ستحدد السياسات التي سيتم وضعها بموجب هذه السياسة الإطارية نطاق وأهداف إدارة أمن المعلومات، وستوفر إطارًا لإدارة أمن المعلومات يحدد مسؤوليات الموظفين والجهات الأخرى ذات الصلة. وتتعهد الشركة باتخاذ التدابير اللازمة لضمان إطلاع موظفيها والجهات التي تربطها بها علاقة عمل على أهداف الشركة والمسؤوليات المتوقعة من أصحاب المصلحة المعنيين لتحقيق هذه الأهداف. وفي هذا الصدد، تلعب السياسات واللوائح المعمول بها دورًا رئيسيًا في إعلام الموظفين وشركاء العمل بالتزاماتهم المتوقعة.

6.3.التدريب والتطوير

6.3.1.تعتبر برامج التدريب والتطوير في مجال إدارة أمن المعلومات ضرورية لتحسين وتعزيز معارف ومهارات موظفي الشركة فيما يتعلق بإدارة أمن المعلومات.

6.3.2.يجب أن يشمل التدريب على إدارة أمن المعلومات مواضيع تتجاوز الوعي الأساسي بالخصوصية والأمن لتطوير أفضل الممارسات ومراقبتها.

يجب على الموظفين فهم قيمة المعلومات ومسؤولياتهم، بما في ذلك جودة البيانات، وأمن المعلومات، وإدارة السجلات، والسرية، وما إلى ذلك.

7.مراقبة الامتثال لسياسة الإطار

7.1.لجنة البيانات الشخصية مسؤولة عن ضمان الامتثال لسياسة الإطار هذه وعن مراجعة وتحديث كل سياسة ذات صلة.

7.2.ينبغي مراجعة السياسات والإجراءات مرة واحدة على الأقل سنويًا. إضافةً إلى ذلك، ينبغي مراجعتها بعد أي تغييرات تؤثر على هيكل النظام أو تقييم المخاطر، ويجب أن تُعتمد أي تغييرات ضرورية من قِبل الإدارة العليا وتُسجل كنسخة جديدة. يجب نشر كل مراجعة بطريقة يسهل الوصول إليها لجميع المستخدمين.

7.3.يتولى مسؤول الاتصال بالبيانات تنظيم اجتماعات مراجعة الإدارة، والتي تُعقد بمشاركة الإدارة العليا ورؤساء الأقسام. تُعقد هذه الاجتماعات، التي يتم خلالها تقييم مدى ملاءمة وفعالية نظام إدارة أمن المعلومات، مرة واحدة على الأقل سنويًا.

8.انتهاك السياسة والعقوبات

إذا تبين أن سياسة ومعايير إطار أمن المعلومات والبيانات الشخصية لم يتم الالتزام بها، فإن الموظفين المسؤولين عن هذا الانتهاك سيخضعون للعقوبات المحددة في البنود ذات الصلة من العقود، والتي تنطبق أيضًا على الأطراف الثالثة، وفقًا للتوجيه والإجراءات التأديبية.