أمن المعلومات
سياسة

IKVKK_P5الإصدار 1.00

شركة كارديلين المحدودة لتجارة صناعة الدهانات والمواد الكيميائية

سياسة أمن المعلومات

1.الهدف:

تُعدّ المعلومات عنصراً أساسياً في دعم جميع أنشطة شركة كارديلين بويا في كيميا ساناي تيكاريت المحدودة. ويُعتبر تأمين جميع المعلومات التي تُعالجها شركتنا أمراً بالغ الأهمية لنجاح عملياتنا الاقتصادية والإدارية. ونسعى إلى تحقيق هذا الهدف من خلال معالجة ثلاثة جوانب أساسية لأمن المعلومات: سرية البيانات، وسلامة البيانات، وإمكانية الوصول إلى البيانات وتوافرها، وهي عناصر حيوية لحماية معلومات الشركة.

أهداف هذه السياسة هي كما يلي:

1.1.يتم حماية موارد المعلومات الخاصة بالشركة بشكل كافٍ ضد الفقدان وسوء الاستخدام والاختراقات.
لتوفير مستوى من الحماية؛

1.2.يوافق جميع المستخدمين على هذه السياسة وغيرها من وثائق السياسة ذات الصلة وقواعد السلوك.
ولضمان إطلاعهم على الإرشادات؛

1.3.يخضع جميع المستخدمين للقانون التركي المعمول به والتزاماتهم في هذا السياق.
لضمان إدراكهم لمسؤولياتهم؛

1.4.رفع مستوى الوعي بين الموظفين وأصحاب المصلحة الآخرين حول الحاجة إلى تنفيذ تدابير أمنية مناسبة في جميع أنحاء الشركة كجزء من هدف التشغيل الفعال ودعم أمن المعلومات؛

1.5.لضمان أن يكون جميع المستخدمين على دراية بمسؤولياتهم فيما يتعلق بسرية وسلامة وتوافر البيانات التي يقومون بمعالجتها؛

ينبغي النظر في هذه السياسة جنبًا إلى جنب مع سياسة معالجة وحماية البيانات الشخصية لشركة Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketiومبادئ التنفيذ ذات الصلة، والتي تحتوي على معلومات مفصلة حول حماية البيانات الشخصية.

2.النطاق:

تغطي هذه السياسة حماية أصول المعلومات الإلكترونية التي يتم الحصول عليها من الأنشطة التجارية التي يتم تنفيذها داخل الشركة وما يتصل بها من أنشطة الخدمات اللوجستية والتخزين والمحاسبة والمالية وضمان الجودة والمشتريات والموارد البشرية والشؤون القانونية والمبيعات والتسويق والتدقيق الداخلي ومعالجة المعلومات، بالإضافة إلى عمليات أمن المعلومات التي تستخدمها شركة Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketiلضمان معالجة وتخزين وحماية وسرية وسلامة البيانات الشخصية المحفوظة داخل الشركة وفقًا للقانون.

2.1. يلتزم جميع موظفي الشركة وجميع الأطراف الثالثة ذات الصلة، بما في ذلك الضيوف المصرح لهم بالوصول إلى المعلومات التي تتحكم بها الشركة أو تُدار نيابةً عنها، بالامتثال لسياسة أمن المعلومات ومبادئ التنفيذ ذات الصلة الواردة في هذه الوثيقة. تغطي أحكام هذه السياسة العمليات التي من خلالها تصل الأطراف المذكورة إلى جميع البيانات والبرامج المملوكة للشركة أو المرخصة لها، وتستخدمها، وذلك عن طريق الاتصال المباشر أو غير المباشر بالشبكات التي توفرها شركة كارديلين بويا في كيميا ساناي تيكاريت المحدودة، باستخدام الأجهزة المملوكة أو المستأجرة أو المعارة من قبل الشركة، وجميع الأدوات والأنظمة الأخرى المقدمة من جهات خارجية، سواء داخل الشركة أو من خلال أنظمة خارجية.

2.2. تنطبق هذه السياسة على جميع البيانات التي تحتفظ بها الشركة، سواء كانت إلكترونية أو مادية، بما في ذلك الطرق المذكورة أدناه:

•البيانات الإلكترونية المخزنة والمعالجة بواسطة أجهزة الكمبيوتر المكتبية والمحمولة والأجهزة الأخرى، بالإضافة إلى أجهزة التخزين؛

•البيانات المنقولة عبر بيئات الشبكة؛

•المعلومات المرسلة باستخدام الفاكس أو طرق نقل مماثلة؛

•جميع السجلات الورقية؛ •المواد المرئية والفوتوغرافية، بما في ذلك الميكروفيش والشرائح وتسجيلات كاميرات المراقبة؛ البيانات الصوتية المتعلقة بالرسائل الصوتية والمحادثات المسجلة، بما في ذلك التواصل وجهاً لوجه؛

2.3. يمكن تصنيف بيانات الشركة بشكل عام إلى بيانات شخصية وبيانات غير شخصية:

•تتم معالجة البيانات الشخصية وفقًا لسياسة معالجة وحماية البيانات الشخصية الخاصة بالشركة وتخضع لأعلى معايير الحماية؛

•تشمل البيانات غير الشخصية الأنواع التالية من البيانات:

فئات خاصة من بياناتك الشركة، بما في ذلك بيانات التخطيط الحساسة تجارياً، والبحوث والبيانات، والبيانات المحمية بموجب اتفاقيات السرية، والبيانات المصنفة قانونياً على أنها بيانات مميزة أو سرية.

تخضع البيانات في هذه الفئة لمستوى عالٍ من الحماية.

ii. بيانات الشركة التي تم نشرها على موقعها الإلكتروني الرسمي، أو غيرها من البيانات التي يجوز نشرها وفقًا للوائح القانونية، مثل قانون حرية المعلومات. من الضروري أن تكون هذه البيانات دقيقة ومحدثة، وأن تكون محمية من الفقدان والوصول غير المصرح به.

2.4. تنطبق أحكام هذه السياسة على جميع مراحل دورة حياة البيانات، بما في ذلك جمع البيانات وتخزينها ومعالجتها وتدميرها.

2.5. على الرغم من أن استخدام منصات التواصل الاجتماعي من قبل موظفينا مجاني وغير خاضع للتنظيم المباشر من قبل الشركة، إلا أن شركتنا تتوقع من موظفيها الامتثال لأحكام هذه السياسة والامتناع عن أي إجراءات قد تضر بسمعة الشركة.

يتطلب ذلك من الأفراد الامتناع عن هذا السلوك. لمزيد من المعلومات حول هذا الموضوع، يرجى مراجعة سياسة وسائل التواصل الاجتماعي.

3.المسؤوليات والصلاحيات:

تُحدد مسؤوليات وصلاحيات الموظفين في توصيفاتهم الوظيفية، إلى جانب مؤهلاتهم وكفاءاتهم. وفيما يلي مسؤوليات الوحدات والأفراد المعنيين في الحفاظ على أنشطة أمن المعلومات وتحسينها:

3.1.رؤساء الأقسام

يتحمل رؤساء الأقسام مسؤولية ضمان امتثال الموظفين وغيرهم من الأفراد المصرح لهم العاملين في الوحدات الخاضعة لإشرافهم للإجراءات والمبادئ، ولا سيما تلك الموضحة في شروط استخدام موارد تكنولوجيا المعلومات.

كما أنهم مسؤولون عن تسجيل موارد المعلومات التي تحتفظ بها الوحدات التي يشرفون عليها في جرد موارد المعلومات الخاصة بالشركة وتعيين مستخدم لموارد المعلومات لكل مورد من موارد المعلومات.

3.2.مستخدمو موارد المعلومات

مستخدمو موارد المعلومات هم المستخدمون المسؤولون عن كل مورد من موارد المعلومات المدرجة في قائمة موارد المعلومات الخاصة بالشركة. ويتحمل هؤلاء المستخدمون مسؤولية إجراء تقييمات سنوية لمخاطر حماية البيانات، وذلك من خلال تقييم المخاطر التي تهدد أمن وسرية موارد المعلومات التي تقع ضمن مسؤوليتهم، واتخاذ التدابير التنفيذية المناسبة.

3.3.موظفونا والأطراف الثالثة المعتمدة

يلتزم جميع موظفي الشركة وجميع الأطراف الثالثة المصرح لها من قبل الشركة بالوصول إلى موارد المعلومات بالامتثال للأحكام المنصوص عليها في هذه السياسة. قبل استخدام أسماء المستخدمين المخصصة لهم بموجب شروط استخدام موارد تقنية المعلومات، يُطلب من جميع الموظفين قبول الشروط والأحكام المحددة تحت العنوان المذكور أعلاه، والتي ستظهر على شاشاتهم. في حالة الكشف عن البيانات أو فقدانها عن طريق الخطأ، أو الوصول غير المصرح به، أو فيروسات الحاسوب، أو البرامج الضارة، أو أي حادث آخر يُعرّض أمن المعلومات للخطر، أو إذا كان يُشتبه في وقوع مثل هذه الحوادث، يجب الإبلاغ عن الوضع فورًا إلى مدير تقنية المعلومات. يمكن للأفراد المعنيين الاتصال بمدير تقنية المعلومات أو موظفيه مباشرةً لهذا الغرض. (انظر القسم 7.1لمعلومات الاتصال).

3.4.مدير تقنية المعلومات

يتولى مدير تكنولوجيا المعلومات مسؤولية الإشراف على موارد تكنولوجيا المعلومات والاتصالات وتنفيذ أنشطة أمن المعلومات اليومية.
يجوز لمدير تكنولوجيا المعلومات تدقيق
جميع الأنظمة المستخدمة لتحديد المخاطر الأمنية والتخفيف من حدتها، أو إزالة أو تعطيل أسماء المستخدمين/تسجيل الدخول والبيانات و/أو البرامج التي تعتبر غير آمنة على الأنظمة الموجودة على الشبكة.

.4الامتثال للتشريعات المعمول بها

.4.1تلتزم شركة كارديلين لتجارة الدهانات والصناعات الكيميائية المحدودة بالامتثال لجميع القوانين واللوائح الإدارية التركية السارية. وفيما يتعلق بأمن المعلومات، فإن العناصر القانونية الأساسية هي القانون رقم 5651بشأن تنظيم المنشورات على الإنترنت ومكافحة الجرائم المرتكبة من خلالها، والقانون رقم 6698بشأن حماية البيانات الشخصية، ولائحة أمن الشبكات والمعلومات في قطاع الاتصالات الإلكترونية.

.4.2يقع على عاتق جميع المستخدمين مسؤولية الامتثال للأحكام القانونية المذكورة آنفًا، وقد تنشأ مسؤولية فردية في حال عدم الامتثال. إذا خالف أي موظف هذه السياسة أو أحكام التشريعات السارية، يجوز اتخاذ إجراءات تأديبية وفقًا لعقد العمل المبرم مع شركتنا واللوائح التأديبية ذات الصلة. قد يؤدي عدم امتثال موردينا أو مقاولينا إلى إنهاء العقد المبرم معنا. وفي بعض الحالات، قد تُتخذ إجراءات قانونية.

.5تأثير جرد بيانات الشركة وحماية البيانات تقييم

.5.1تحتفظ شركة كارديلين للدهانات والصناعات الكيميائية المحدودة بسجل بيانات يتضمن تفاصيل حول مصادر البيانات المستخدمة داخل الشركة. ويتولى رؤساء الأقسام ومديرو الفروع مسؤولية تعيين مستخدم موارد لكل مصدر معلومات تحتفظ به وحداتهم، وتسجيل هذه المعلومات في سجل بيانات الشركة.

.5.2سيُجرى تقييم سنوي للأثر لجميع مصادر المعلومات المستخدمة، فيما يتعلق بمخاطر خصوصية البيانات وأمنها، والمخاطر التي قد تُشكلها الأدوات المستخدمة على حق الأفراد في الخصوصية. كما سيُجرى تقييم للأثر قبل استخدام أي مصادر معلومات جديدة. وستُحدد التدابير المتخذة للتخفيف من هذه المخاطر بالنسبة للمصادر التي تعالج البيانات المصنفة ضمن فئات البيانات الخاصة، وذلك في قائمة جرد البيانات.

.6مراقبة الاتصالات الإلكترونية

وفقًا للمادة 6من القانون رقم 5561بشأن تنظيم المنشورات على الإنترنت ومكافحة الجرائم المرتكبة من خلالها، بعنوان "التزامات مزود خدمة الوصول"، تتخذ الشركة التدابير اللازمة لتخزين معلومات حركة الاتصالات الإلكترونية الواردة أو المرسلة من قبلها، وذلك في حدود الأغراض المحددة في القانون، ولضمان دقة هذه المعلومات وسلامتها وسريتها. ويشمل ذلك، على سبيل المثال لا الحصر، مراقبة ما إذا كانت المعلومات تُستخدم لأغراض إجرامية أو غير مصرح بها، وإجراء عمليات تدقيق وتدخلات لحماية النظام من التهديدات كالفيروسات والاختراق وهجمات حجب الخدمة، وضمان امتثال عمليات تقنية المعلومات لسياسات الشركة وتوجيهاتها.

ولا تقتصر هذه الإجراءات على ما سبق. سيتم تنفيذ إجراءات التفتيش وفقًا لمبادئ التنفيذ المتعلقة بالاتصالات الإلكترونية وفحص البيانات.

7.الأحداث المتعلقة بأمن البيانات

7.1.إذا اكتشف أي مستخدم أو اشتبه في حدوث خرق لأمن البيانات أو إساءة استخدام موارد المعلومات التي تنتهك سرية البيانات وإمكانية الوصول إليها وسلامتها، فسوف يقوم بإبلاغ فريق دعم قسم تكنولوجيا المعلومات.

7.2.إذا كان خرق أمن البيانات ينطوي على التدمير العرضي أو غير القانوني أو الفقدان أو التغيير أو الوصول غير الفعال إلى البيانات الشخصية أو الكشف عن البيانات الشخصية لأطراف غير مصرح لها، فيجب على المستخدمين إعداد وإرسال تقرير إخطار خرق أمن البيانات على الفور، والمرفق كملحق لخطة الاستجابة لخرق البيانات، إلى مسؤول الاتصال بحماية البيانات / المدير.

معلومات الاتصال بمسؤول/مدير الاتصال بحماية البيانات: شركة كارديلين المحدودة لتجارة صناعة الدهانات والكيماويات

رقم الهاتف: 33 11 398 312 90+
فاكس: 11 09 398 312 90+
البريد الإلكتروني: kvkk@kardelenboya.com.tr

7.3.في حالة وقوع حادثة أمنية تتعلق بالبيانات، أو عند الاشتباه في وقوعها، يجوز لمدير تكنولوجيا المعلومات اتخاذ تدابير فورية لحل الحادثة أو التخفيف من الأضرار المحتملة، مثل حظر وصول المستخدم إلى النظام أو فحص الأجهزة المتصلة بالشبكة.

7.4.قد يؤدي رفض الإبلاغ عن حادثة أمنية متعلقة بالبيانات أو خرق للبيانات الشخصية إلى إجراء تحقيق بموجب اللوائح التأديبية. في حال وجود أي تردد في الإبلاغ عن الحادثة، يمكن استشارة مدير تقنية المعلومات أو مسؤول/مدير الاتصال بحماية البيانات.

8.التدريب على أمن البيانات

8.1.يجب على الموظفين الذين سيستخدمون معدات تقنية المعلومات لأول مرة، والجهات الخارجية المصرح لها بالوصول إلى هذه المعدات، الإلمام بسياسات وإجراءات أمن المعلومات الخاصة بالشركة. علاوة على ذلك، قبل منح الوصول إلى خدمات تقنية المعلومات، يجب تدريب المستخدمين على متطلبات أمن عملهم، وبشكل عام، على الاستخدام الأمثل لأصول تقنية المعلومات الخاصة بالشركة. تقع على عاتق المديرين مسؤولية ضمان تدريب الموظفين بشكل صحيح، والاحتفاظ بسجلات التدريب. يجب إبلاغ المستخدمين بهذه السياسة، بما في ذلك إجراءات الإبلاغ الواردة في القسم 7.

8.2.سيخضع جميع موظفي الشركة لتدريب على التوعية بأمن المعلومات وحماية البيانات الشخصية، وسيُعقد هذا التدريب إلكترونياً أو حضورياً. ومن المقرر أن يصبح هذا التدريب إلزامياً في المستقبل.

9.التقييمات الأمنية في مجال التوظيف

9.1.ينبغي تضمين الأدوار والمسؤوليات التي يتعين القيام بها فيما يتعلق بالأمن، كما هو محدد في هذه السياسة واللوائح ذات الصلة، في توصيفات الوظائف عند الاقتضاء.
ينبغي أن تشمل هذه المسؤوليات العامة لتنفيذ سياسة الأمن، بالإضافة إلى مسؤوليات حماية أصول المعلومات المحددة أو تنفيذ عمليات أو أنشطة الأمن.

9.2.بما أن السلطة والمسؤوليات المتعلقة بأمن البيانات قد تتغير في حالات طلبات التوظيف أو تغييرات وظائف الموظفين، فيجب تقييم هذه الأمور من قبل قسم الموارد البشرية.

9.3.سيُطلب من موظفي الموردين أو المقاولين ومستخدمي الطرف الثالث الذين سيستخدمون أنظمة المعلومات الخاصة بالشركة توقيع اتفاقيات سرية كجزء من عقودهم، وإذا كان لديهم حق الوصول إلى البيانات الشخصية التي تحتفظ بها الشركة، فسيكون مطلوبًا منهم توقيع اتفاقيات مشاركة البيانات.

10.حماية بيانات الفئات الخاصة

تتخذ الشركة إجراءات أمنية أقوى لحماية البيانات الشخصية الحساسة. يُعدّ تنفيذ البند 10.1أمراً ضرورياً.

10.2. لا ينبغي تخزين أو نقل فئات البيانات الخاصة في عناوين البريد الإلكتروني الفردية (Gmail، Hotmail، إلخ) أو خدمات التخزين السحابي المستندة إلى الويب (Google Apps، Dropbox، إلخ) التي لا توفرها الشركة.

(بما في ذلك 10.3 قواعد البيانات وأجهزة الكمبيوتر التي تحتوي على بيانات حساسة، ويجب أن تتطلب من المستخدمين إدخال بيانات الاعتماد للوصول إلى البيانات

حيثما أمكن، ينبغي إخفاء هوية البيانات أو استخدام أسماء مستعارة لحماية الهويات، وخاصة عند التعامل مع بيانات المرضى/المشاركين القابلة للتحديد.

10.4.يجب مسح جميع البيانات الموجودة على الأجهزة التي تستخدمها شركتي بشكل آمن عند التخلص منها.

10.5. يجب تشفير ملفات البيانات سواء في الوسائط التي يتم تخزينها فيها أو أثناء نقلها.

11.شروط استخدام موارد تكنولوجيا المعلومات

11.1. يُعتبر أي شخص يستخدم موارد تكنولوجيا المعلومات الخاصة بالشركة قد قبل ما يلي:

تشير موارد تكنولوجيا المعلومات إلى جميع الأجهزة والبرامج والخدمات والموارد المُقدمة لتشغيل الشركة. ويشمل ذلك جميع شبكات الحاسوب والاتصالات السلكية، وما إلى ذلك.

أو تُعتبر أجهزة الكمبيوتر اللاسلكية والطابعات والأجهزة المحمولة وأجهزة التخزين وأنظمة الصوت والصورة والخدمات السحابية ضمن موارد تكنولوجيا المعلومات. 11.2.

ينبغي على كل مستخدم أن يفهم ويطبق النصائح المقدمة بشأن الاستخدام الآمن لموارد تكنولوجيا المعلومات، وأن يحضر دورات تدريبية للتوعية بأمن المعلومات، وأن يكون على دراية ببيان التوعية بأمن المعلومات؛ 11.3.

يجب أن يقتصر استخدام موارد تقنية المعلومات الخاصة بالشركة، واستخدامها لتوفير الوصول إلى موارد خارجية، على البحث والتعلم والإدارة والاستخدامات الأخرى المسموح بها والضرورية لعمليات الشركة. يُحظر استخدام موارد تقنية المعلومات لأغراض تجارية شخصية دون إذن مسبق. 11.4. يجب تنفيذ الأنشطة نيابةً عن الشركة باستخدام أدوات معالجة المعلومات التي توفرها الشركة فقط. يُحظر استخدام خدمات المعلومات الخارجية لإدارة أعمال الشركة، لما في ذلك من مخاطر تُعرّض بيانات الشركة للخطر، إلا في حال وجود مبرر كافٍ. على سبيل المثال، يجب استخدام خدمة البريد الإلكتروني الخاصة بالشركة بدلاً من Dropbox أو OneDrive أو خدمات البريد الإلكتروني الأخرى مثل Hotmail وGmail. 11.5.

يُسمح باستخدام موارد تقنية المعلومات الخاصة بالشركة للأغراض الشخصية فقط إذا لم يتعارض ذلك مع أعمال الشركة وعملياتها أو مع أداء مهام المستخدمين الآخرين. ويخضع استخدام شبكة الواي فاي الخاصة بالشركة لأغراض الترفيه لهذا الشرط أيضًا.

يُحظر توصيل الموزعات ونقاط الوصول اللاسلكية وأجهزة التوجيه توصيل أجهزة الشبكة النشطة بشبكة الشركة. سيتم تخصيص جميع عناوين IP وإدارتها مركزيًا من قبل الشركة.

11.7. يُحظر على الضيوف الخارجيين وما شابههم الوصول إلى خدمات تقنية المعلومات الخاصة بالشركة؛ 11.8. يلتزم كل مستخدم لموارد تقنية المعلومات الخاصة بالشركة

لا يجوز للموظفين مغادرة الشركة إلا بإذن كتابي صريح مسبق.

بالامتثال لسياسة أمن المعلومات الخاصة بالشركة، بما في ذلك شروط استخدام موارد تقنية المعلومات وجميع الأحكام واللوائح والقواعد والأنظمة القانونية وغيرها من الأحكام ذات الصلة. وعلى وجه الخصوص، لا الحصر، يلتزم كل مستخدم بالتصرف وفقًا لما هو منصوص عليه في البنود التالية:

11.8.1. لا تفصح عن كلمة المرور واسم المستخدم اللذين خصصتهما لك الشركة لأي شخص.

11.8.2. لن يُسمح بالوصول إلى موارد تكنولوجيا المعلومات، سواء داخل الشركة أو خارجها، إلا للأغراض المصرح بها، ولن يتم تسهيل الوصول إلى هذه الموارد لأغراض غير مصرح بها من قبل أفراد آخرين؛

11.8.3. لا يجوز استخدام أو إدخال أي مواد أو موارد إلى الشبكة من شأنها أن تسمح بالوصول غير المصرح به أو التعديل أو تعطيل أي مورد من موارد تكنولوجيا المعلومات، مثل فحص المنافذ، داخل الشركة أو في أي مكان آخر؛ 11.8.4. أي شيء يمكن اعتباره مسيئًا أو ضارًا بسمعة الشركة.

لا يجوز عرض أو تخزين أو استقبال أو نقل الصور أو النصوص التي تحتوي على مواد مرئية أو صوتية إباحية أو متعلقة بالتحرش بالأطفال أو جنسية أو عنصرية أو تشهيرية أو تهديدية أو قذفية أو غير قانونية أو تمييزية أو إرهابية والتي قد تضر بالآخرين؛ 11.8.5. لا يجوز انتحال توقيعات و/أو رؤوس البريد الإلكتروني، ولا يجوز إنشاء و/أو إرسال رسائل بريد إلكتروني "متسلسلة" أو "غير مرغوب فيها" أو "مضايقة"، ولا يجوز استخدام انتحال الشخصية للتصرف نيابة عن الآخرين في الاتصالات الإلكترونية، ولا يجوز إنشاء اتصالات غير ضرورية أو مسيئة؛

11.8.6.يجب تشفير جميع الأجهزة المحمولة المستخدمة للوصول إلى الموارد التي توفرها الشركة كجزء من خدمات تكنولوجيا المعلومات الخاصة بها باستخدام برامج التشفير المناسبة وحمايتها برمز PINأو كلمة مرور؛

11.8.7.جميع المواد والبرامج التي توفرها الشركة والأطراف الثالثة

سيتم احترام حقوق التأليف والنشر، ولن يتم استخدام المواد المحمية بحقوق التأليف والنشر، بما في ذلك البرامج والبيانات المكتسبة، أو تنزيلها أو نسخها أو تخزينها على النظام أو توريدها إلا بإذن من صاحب حقوق التأليف والنشر أو بموجب شروط الترخيص الذي تحتفظ به الشركة؛ 11.8.8.عند معالجة البيانات المتعلقة بالأشخاص الطبيعيين، سيتم الالتزام بأحكام تشريعات حماية البيانات.

سيتم اتباع سياسة حماية البيانات الخاصة بالشركة لمعالجة البيانات (أي جمعها واستخدامها ومشاركتها وإتلافها) بشكل مناسب. 11.8.9.البيانات التي يُنشئها المستخدمون/البيانات المملوكة لهم/البيانات التي يمتلكها المستخدمون على موارد تكنولوجيا المعلومات الخاصة بالشركة

تجدر الإشارة إلى أن جميع أصول المعلومات المخزنة قد تخضع للتدقيق من قبل الشركة أو السلطات القانونية في حال وجود شبهة بارتكاب أفعال محظورة. وفي حال تشفير البيانات ذات الصلة، يُطلب من المستخدم تقديم مفتاح فك التشفير؛ 11.8.10.يجب تحديد شروط ترخيص جميع المواد والبرامج المستخدمة عبر أي منصة والعمل بموجبها؛ 11.9.وفقًا للمادة 6من القانون رقم 5561بشأن تنظيم النشر على الإنترنت ومكافحة الجرائم المرتكبة من خلاله، تتخذ الشركة التدابير اللازمة لتخزين معلومات حركة الاتصالات الإلكترونية التي تتلقاها أو ترسلها، بما يقتصر على الأغراض المنصوص عليها في القانون، ولضمان دقة هذه المعلومات وسلامتها وسريتها. وتُنظم إجراءات تنفيذ هذه التدابير بموجب مبادئ التنفيذ الخاصة بالاتصالات الإلكترونية وتدقيق البيانات.

[illegible] اتخاذ تدابير على الفور لحل

11.11.إذا لزم إجراء مزيد من التحقيق، فسيتصل قسم تكنولوجيا المعلومات بالشركة.

بموافقة صريحة من مجلس الإدارة، يجوز للشركة اتخاذ الإجراءات اللازمة لفحص أي نظام على شبكتها. 11.12.

باستثناء ما يقتضيه القانون المعمول به، لن تكون الشركة مسؤولة عن أي خسارة أو ضرر أو حدث سلبي ينشأ بشكل مباشر أو غير مباشر عن استخدام أو منع استخدام أي موارد تكنولوجيا المعلومات التي توفرها و/أو تديرها.

11.13.على الرغم من أن الشركة ليست مسؤولة عن الوصول غير المصرح به إلى البيانات الشخصية وغيرها من البيانات أو تعديلها.

مع أن المزود يتخذ التدابير الأمنية المناسبة ضد إفشاء البيانات أو إتلافها أو فقدانها العرضي، إلا أنه لا يقدم أي ضمان أو كفالة للمستخدم فيما يتعلق بأمن البيانات أو سريتها أو سلامتها. 11.14.

سيتم تخزين اسم المستخدم وعنوانه وصورته وحالته الاجتماعية وعنوان بريده الإلكتروني واسم تسجيل الدخول ولقبه وبطاقة هوية الشركة وغيرها من المعلومات ذات الصلة في وسائط معالجة الكمبيوتر لاستخدامها في أغراض أخرى مثل إدارة ومراقبة استخدام النظام.

11.15. تنطبق الشروط المذكورة أعلاه أيضاً على استخدامات شبكة الشركة من قبل الأجهزة غير المملوكة للشركة، مثل أجهزة الكمبيوتر المحمولة الشخصية وأجهزة الكمبيوتر المنزلية، عند اتصالها بشبكة الشركة مباشرةً و/أو عبر شبكة VPN. 11.16.

قد يؤدي انتهاك الشروط المذكورة أعلاه إلى اتخاذ إجراءات تأديبية، بما في ذلك تعليق الوصول إلى جميع موارد تقنية المعلومات الخاصة بالشركة لفترات محددة و/أو فرض غرامات. في حالات الانتهاكات الجسيمة، تحتفظ الشركة بحقها في إنهاء عقد العمل مع الطرف المعني واتخاذ الإجراءات المدنية والجنائية ضد المستخدم. سيعمل موظفو الشركة كوكلاء للضيوف الذين يستخدمون مرافق تقنية المعلومات الخاصة بالشركة و/أو خدمة الإنترنت التي توفرها الشركة. يجب على الموظفين الذين يعملون كوكلاء مراقبة تصرفات ضيوفهم وتحمل مسؤوليتها.