نقل البيانات
إجراءات الأمن و
حول مبادئها
أنظمة

IKVKK_Y8الإصدار 1.00

شركة كارديلين المحدودة لتجارة صناعة الدهانات والمواد الكيميائية

إجراءات ومبادئ أمن نقل البيانات
اللوائح المتعلقة بـ

1.الغرض والنطاق

تخزن شركتنا كمية كبيرة من البيانات، إلكترونياً وورقياً، في إطار أنشطتها الاقتصادية. وتهدف هذه اللائحة الخاصة بإجراءات ومبادئ أمن نقل البيانات (المشار إليها فيما يلي بـ "اللائحة") إلى تنظيم الإجراءات المطبقة لحماية البيانات المخزنة وضمان النقل الآمن للبيانات الشخصية داخل الشركة وخارجها.

ينطبق هذا النظام على جميع الفئات التالية من الأفراد داخل شركتنا الذين يقومون بمعالجة البيانات الشخصية والبيانات الشخصية الحساسة، والذين يُطلب منهم نقل هذه البيانات إلى أصحاب المصلحة في الشركة كجزء من واجباتهم:

•الموظفون •الموردون والمقاولون الذين تتعاون معهم شركتنا •المتدربون

ينبغي على موظفينا النظر في هذا النظام جنباً إلى جنب مع النظام المتعلق بالإجراءات والمبادئ الخاصة باستخدام تكنولوجيا المعلومات والاتصالات وسياسة أمن المعلومات.
ينبغي عليهم شراؤه.

2.التشريعات ذات الصلة

القانون رقم 6698بشأن حماية البيانات الشخصية واللوائح الإدارية ذات الصلة.

3.بيانات الفئة الخاصة

لأغراض هذا النظام، تشمل الفئات الخاصة من البيانات فئات البيانات التالية:

•البيانات المتعلقة بعرق الشخص، وأصله العرقي، وآرائه السياسية، ومعتقداته الفلسفية، ودينه، وطائفته أو معتقداته الأخرى، ومظهره وملابسه، وعضويته في الجمعيات أو المؤسسات أو النقابات العمالية، وصحته، وحياته الجنسية، وإداناته الجنائية، وتدابيره الأمنية، بالإضافة إلى البيانات البيومترية والوراثية.

•بيانات سرية تعتبرها شركتنا أسرارًا تجارية. •بيانات سرية في العقود المتعلقة بالسلع والخدمات والمنتجات.

جميع البيانات المحددة.

•بيانات سرية تتعلق بعملاء وموردي شركتنا.

يجب على أي موظف لديه أي شكوك حول ما إذا كانت أي بيانات تتم معالجتها تشكل بيانات من فئة خاصة أن يبلغ رئيس القسم المعني بذلك وأن يتصرف وفقًا لتعليماته.

.4الاعتبارات أثناء نقل البيانات

النقاط الأساسية

.4.1عند نقل البيانات الشخصية والبيانات الشخصية الحساسة، يجب على كل موظف التشاور مع رئيس القسم ذي الصلة للحصول على إذن بنقل البيانات وتقديم التعليمات.

.4.2يجب نقل الفئات الخاصة من البيانات الشخصية وغيرها من البيانات الشخصية فقط بالقدر الضروري تمامًا للسير السليم للأنشطة القانونية لشركتنا.

وبناءً على ذلك، قبل كل عملية نقل بيانات، يجب تحديد ما إذا كانت عملية نقل البيانات ضرورية أم لا.

.4.3عند التواصل مع أطراف ثالثة، ينبغي التأكد من وجود اتفاقيات لتبادل البيانات وبروتوكولات إضافية لحماية البيانات الشخصية موقعة مع الأطراف المعنية. كما ينبغي التحقق من وجود بند يتعلق بأساليب نقل البيانات المقترحة، وفي حال وجوده، يجب توخي الحذر عند استخدام هذه الأساليب.

.4.4يجب التحقق دائمًا من عدم تقديم معلومات تتجاوز ما هو ضروري للغرض المحدد. على سبيل المثال، إذا طُلب قسم أو جزء محدد من مستند، فلا ينبغي إرسال المستند أو المخطط بأكمله.

.4.5في جميع الحالات التي يتم فيها نقل البيانات الشخصية والمعلومات التي تحتوي على فئات خاصة من البيانات الشخصية، يجب تحديد هوية المتلقي وتفويض الوصول إلى البيانات بشكل واضح.

.5طرق نقل البيانات

قبل تحديد طرق نقل البيانات، ينبغي مراعاة النقاط التالية:

•طبيعة المعلومات المراد نقلها، وحساسيتها، ومستوى سريتها، أو احتمالية
قيمة
•حجم البيانات المراد نقلها •الخسائر التي قد تلحق بالأفراد المعنيين نتيجة لنقل البيانات

الخسائر أو الصعوبات المحتملة التي قد تبقى
•عواقب فقدان البيانات على شركتنا. •يجب عدم نقل المعلومات والوثائق التي تتجاوز ما هو ضروري للغرض المحدد. يجب تنقيح جميع البيانات غير الضرورية أو إزالتها بالكامل قبل النقل عند الضرورة.

.5.1نقل البيانات عبر البريد الإلكتروني

•لا ينبغي استخدام البريد الإلكتروني لنقل البيانات الحساسة غير المشفرة التي قد تحتوي على معلومات شخصية. يجب أن يدرك موظفونا أن البريد الإلكتروني غير مصمم لإرفاق ونقل كميات كبيرة من البيانات.

ينبغي على موظفينا تفضيل استخدام طرق آمنة بديلة لنقل البيانات الحساسة كلما أمكن ذلك. وفي حال عدم توفر بديل مناسب، ينبغي استخدام مستويات أمان إضافية.

على سبيل المثال، ينبغي استخدام التشفير، أو اشتراط كلمات المرور وأسماء المستخدمين للوصول إلى البيانات الحساسة المراد إرسالها. عند نقل أسماء المستخدمين وكلمات المرور، يُنصح باستخدام وسائل بديلة كالبريد الإلكتروني، أو المكالمات الهاتفية إلى أرقام محددة، أو الرسائل النصية القصيرة. •في رسائل البريد الإلكتروني، يجب تقديم تعليمات واضحة بشأن المسؤوليات القانونية للمستلم الذي استلم البيانات عن طريق الخطأ، وما يجب عليه فعله بالبريد الإلكتروني الوارد في حال لم يكن المستلم هو الشخص الصحيح. •عند الاقتضاء، يجب إرفاق المعلومات المرسلة في ملفات مغلقة.

ينبغي إرسالها.

•يجب الحرص على التأكد من دقة المعلومات الواردة في عنوان البريد الإلكتروني أو محتواه. ولا يجوز الكشف عن كامل محتوى المرفقات أو البيانات الشخصية الحساسة في اسم الملف أو عنوان البريد الإلكتروني. •يجب إرسال رسائل البريد الإلكتروني إلى الشركة مع تضمين معلومات الخصوصية والأمان المناسبة.

يجب إرسالها باستخدام عنوان البريد الإلكتروني المقدم.

5.2.بوابة الشركة الداخلية

•يجب على المستخدمين الذين يحتاجون إلى نسخ أو نقل البيانات إلى وسيط قابل للإزالة، أو الذين لديهم كمية كبيرة جدًا من البيانات لإرسالها، طلب المساعدة من فريق دعم تكنولوجيا المعلومات بالشركة.

•لا يجوز الوصول إلى البوابة باستخدام مستكشف الملفات دون الحصول على إذن مسبق من فريق دعم تقنية المعلومات. •عند تحميل البيانات إلى البوابة، تأكد من تسمية الملفات بشكل صحيح وتخزينها في المواقع المناسبة. يجب عدم تخزين البيانات المتخصصة التي تتطلب التحميل إلى البوابة في مواقع متاحة للعامة.

•عند تحميل البيانات إلى شبكة الشركة، يجب الحرص على استخدام بوابة آمنة باتباع الإجراءات المناسبة.

•يجب تشفير كل جزء من البيانات المراد نقلها إلى الموارد التعليمية عبر الإنترنت باستخدام مستند محمي بكلمة مرور أو ملف مضغوط مشفر.

5.3.أجهزة تخزين البيانات القابلة للإزالة (بطاقة الذاكرة، محرك أقراص USB، إلخ).

يجب تشفير جميع البيانات المنقولة عبر وسائط تخزين قابلة للإزالة، مثل أجهزة الذاكرة المحمولة USB. ويجب حماية أجهزة التخزين المحمولة المشفرة بكلمات مرور قوية. وفي حال الحاجة إلى الكشف عن كلمة المرور لطرف ثالث، فينبغي إرسال هذه المعلومات عبر وسائل بديلة، مثل البريد أو الهاتف أو الرسائل النصية القصيرة.

•يجب على المستخدمين الذين يحتاجون إلى نسخ أو نقل البيانات إلى وسائط قابلة للإزالة، أو الذين لديهم كمية كبيرة جدًا من البيانات لإرسالها، طلب المساعدة من فريق دعم تكنولوجيا المعلومات بالشركة.

•يجب تحديد ملكية الوسائط القابلة للإزالة المستخدمة بوضوح. يجب إعادة الوسائط القابلة للإزالة إلى مالكها بعد نقل البيانات، ويجب حذف البيانات المنقولة من جهاز تخزين البيانات بعد الاستخدام.

•في الحالات التي لا يكون فيها المستلم هو الشخص الصحيح ويتم نقل البيانات عن طريق الخطأ، يجب تقديم تعليمات واضحة بشأن المسؤوليات القانونية للمستلم وما يجب فعله بالبريد الإلكتروني الوارد.

•الكشف عن معلومات حول محتويات الملف المشفر في اسم الملف والرسائل المرفقة.
لا ينبغي فعل ذلك.

•يجب على المرسل أن يؤكد في الوقت المناسب ما إذا كان نقل البيانات قد تم بنجاح وأن يصدر إيصالاً لهذا الغرض.

قد تكون رسائل البريد الإلكتروني التي تؤكد استلام الملف مناسبة لهذا الغرض. •يجب الإبلاغ عن أي مشاكل إلى المشرفين المباشرين، وإبلاغ مسؤول حماية البيانات/مسؤول الاتصال فورًا عن أي بيانات مفقودة أو تالفة.

.5.4المكالمات الهاتفية

نظراً لإمكانية مراقبة المحادثات الهاتفية أو سماعها أو مقاطعتها (عمداً أو عن طريق الخطأ)، ينبغي اتخاذ الاحتياطات التالية:

•لا ينبغي نقل البيانات الشخصية أو مناقشتها عبر الهاتف إلا بعد التحقق من هوية المستلم وتفويضه.

•عند استخدام جهاز الرد الآلي، لا تترك رسائل حساسة أو سرية أو تُدرج أي بيانات شخصية. وفّر وسيلة للتواصل فقط، وتوقع من المُستلم التحدث معك شخصيًا.

•أثناء استماعك لرسائل البريد الصوتي التي تُركت لك، قد يكون الآخرون يتنصتون.
احرص على عدم تشغيل التسجيل الصوتي في المناطق المفتوحة حيث يوجد خطر وقوع حوادث.

.5.5نقل البيانات عبر البريد وخدمات التوصيل

•لنقل البيانات على وسائط تخزين مادية مثل بطاقات الذاكرة أو الأقراص المدمجة، يُنصح باستخدام خدمات البريد الآمنة. ويُفضل استخدام خدمات البريد المسجل أو خدمة التوصيل السريع على خدمات البريد العادية. في حال استخدام خدمات بريدية أخرى غير البريد التركي ،(PTT)يُنصح باختيار شركات تقدم خدمات توصيل آمنة تتطلب توقيعًا عند التسليم.

يجب ذكر اسم المستلم بوضوح في نموذج الشحن البريدي، كما يجب تصميم غلاف الشحنة بشكل آمن لمنع الكسر أو التلف. ينبغي إبلاغ المستلمين مسبقًا بموعد استلام البيانات. يجب على المستلم تأكيد استلام البيانات بشكل آمن فور وصولها. يلتزم المرسل المسؤول عن نقل البيانات بتأكيد استلامها بشكل آمن.

.5.6التسليم باليد

يُعدّ التسليم والاستلام اليدوي للوثائق من بين طرق النقل المعتمدة. إذا كان من المقرر أن يستلم شخص ما البيانات المراد نقلها، فيجب التحقق من هويته مسبقًا، واستخدام وسائل التحقق المناسبة من الهوية وقت التسليم للتأكد من أن المستلم هو الشخص المقصود.

6.البيانات المفقودة

عندما يكتشف أي موظف فقدان أي بيانات، يجب عليه إبلاغ مشرفه المباشر ومسؤول حماية البيانات/مسؤول الاتصال على الفور، ويجب تنفيذ الإجراءات المحددة في لائحة خطة الاستجابة لخرق البيانات الشخصية دون تأخير.

إذا كان هناك اشتباه في أن مستخدمين غير مصرح لهم قد تمكنوا من الوصول إلى بيانات شخصية حساسة، فيجب إخطار جهات إنفاذ القانون على الفور.

7.الإهمال في إجراءات نقل البيانات

قد يُعتبر الموظفون الذين لا يلتزمون بأحكام هذه اللائحة مُقصّرين في أداء واجباتهم، وقد يتم إنهاء عقود عملهم. كما قد تؤدي انتهاكات البيانات الشخصية إلى فقدان شركتنا للتواصل مع العملاء وفرض غرامات باهظة عليها.

لذلك، يجب على موظفينا توخي أقصى درجات الحذر عند نقل البيانات الشخصية الحساسة.

إنه أمر ضروري. تشمل الإجراءات التي قد تُعتبر إهمالاً وسلوكاً خاطئاً ما يلي: نقل البيانات بدون ترخيص، وعدم تشفير البيانات بشكل صحيح، وعدم استخدام الحماية من الضغط والتشفير، وعدم استخدام الخدمات البريدية المسجلة أو المؤمن عليها، وما إلى ذلك.