قبول الإنترنت وأدوات الاتصال الإلكترونية

الاستخدامات المحتملة

السياسة المتعلقة بالإجراءات والمبادئ

IKVKK_P9الإصدار 1.00

شركة كارديلين المحدودة لتجارة صناعة الدهانات والمواد الكيميائية

أدوات الاتصال عبر الإنترنت والإلكترونيات
إجراءات الاستخدام المقبول
السياسة المتعلقة بالمبادئ

1.مقدمة

تلتزم شركة كارديلين بويا في كيميا ساناي تيكاريت المحدودة، بصفتها كيانًا قانونيًا خاصًا، بضمان الاستخدام الأمثل لجميع موارد الشركة المخصصة لها، ومنع إساءة استخدامها أو استخدامها بشكل غير لائق يتعارض مع الغرض المقصود منها. وتشمل هذه المسؤولية استخدام خدمات مثل البريد الإلكتروني والإنترنت.

2.الغرض والنطاق

تهدف هذه السياسة إلى تحديد الإجراءات والمبادئ التي يجب على موظفي شركتنا الالتزام بها عند استخدام وسائل الاتصال الإلكترونية مثل الإنترنت والبريد الإلكتروني. تتكون هذه السياسة من ثلاثة أجزاء:

•سياسة استخدام الإنترنت •سياسة استخدام البريد الإلكتروني

•الاتصالات الإلكترونية بين الموظفين

ينبغي النظر في هذه السياسة بالتزامن مع وثائق السياسة التالية:

•لوائح تأديب الشركة

•سياسة حماية البيانات ومعالجتها •سياسة أمن المعلومات

لأغراض هذه السياسة، تُفسَّر جميع أشكال الاتصال الإلكتروني، بما في ذلك البريد الإلكتروني، والبريد الإلكتروني عبر الإنترنت، والرسائل الفورية، ومنتديات الإنترنت، على أنها تشمل جميع أشكال الاتصال الإلكتروني. إذا استُخدمت خدمات الإنترنت والبريد الإلكتروني التي توفرها الشركة عبر شبكة لاسلكية داخل مبنى الشركة أو عبر الوصول إليها من خارجه، يُعتبر ذلك بمثابة قبول من الطرف المعني لأحكام هذه التعليمات.

3.سياسة استخدام الإنترنت

3.1.أغراض تقديم الخدمة ومسؤوليات المستخدم:

تُقدَّم خدمة الإنترنت في المقام الأول ولأغراض العمليات التجارية للشركة. ويُسمح بالاستخدام الفردي شريطة أن يكون معقولاً ومراعياً ومُتّبعاً للمسؤولية، لا سيما عندما يستخدم الموظفون الإنترنت لأغراض شخصية.

3.2. مراقبة الاستخدام:

3.2.1. لا يوجد توقع معقول للخصوصية أو السرية للموظفين الذين يستخدمون شبكة الإنترنت الخاصة بالشركة. تستخدم الشركة مواقع وروابط شبكة آمنة لتسجيل عمليات البحث على الإنترنت ومنع الوصول غير المصرح به من قبل الموظفين.

يستخدم النظام الخدمات التالية . ويتولى مدير تقنية المعلومات إدارة النظام، بينما يشرف عليه رؤساء الأقسام ومجلس الإدارة. ويتم اختبار جدار الحماية دوريًا لتحديد أي قصور أو ثغرات محتملة في النظام.

3.2.2. برنامج المراقبة: يراقب البرنامج استخدام شبكة الإنترنت الخاصة بالشركة، ويقوم قسم تقنية المعلومات ورؤساء الأقسام بمراقبة سجلات الشبكة ومراجعتها لضمان الاستخدام وفقًا لسياسات الشركة. يشمل ذلك فحص شاشات الكمبيوتر عن بُعد، والتحقق من الملفات ورسائل البريد الإلكتروني، وتحليل المواقع الإلكترونية التي تمت زيارتها. يسجل البرنامج جميع المواقع الإلكترونية التي تمت زيارتها، بالإضافة إلى اسم المستخدم وتاريخ ووقت الزيارة، ويُصدر تقارير دورية لأغراض المراقبة. سيتم الإبلاغ تلقائيًا عن الزيارات والمواقع الإلكترونية المشبوهة أو المسيئة، وسيتم اتخاذ الإجراءات التأديبية المعتادة. بمجرد دخول المستخدمين إلى شبكة الإنترنت الخاصة بالشركة، يُعتبرون موافقين على أنشطة المراقبة والتحكم في الوصول إلى الإنترنت الموضحة أعلاه.

3.3. الاشتراك الشخصي والاستخدام الترفيهي:

لا يجوز للموظفين الاشتراك في خدمات الإنترنت أو الخدمات الإلكترونية داخل الشركة واستخدامها على أجهزة الكمبيوتر الخاصة بالشركة إلا بموافقة خطية من مدير تقنية المعلومات. كما لا يجوز لهم استخدام خدمة الإنترنت لأغراض ترفيهية غير لائقة، مثل ألعاب الكمبيوتر أو المقامرة.

3.4. الإجراءات التي قد تضر بسمعة الشركة:

لا يجوز للموظفين استخدام الإنترنت بطريقة تتعارض مع مصالح الشركة أو تُلحق الضرر بها أو بشركائها أو بسمعتها. على سبيل المثال، الاشتراك في مواقع إلكترونية تحتوي على مواد محظورة أو غير قانونية، أو استخدام أو تحميل محتوى محمي بحقوق الطبع والنشر من جهات خارجية دون الحصول على إذن صريح من صاحب حقوق الطبع والنشر.

3.5. تثبيت البرنامج (التنزيل):

لتقليل مخاطر الفيروسات ومنع وجود برامج غير مرخصة على الشبكة، يُحظر تثبيت أي برامج باستخدام شبكة الشركة. يشمل هذا الحظر أيضًا برامج الألعاب وشاشات التوقف. في حال الحاجة إلى استثناء من هذا الحظر لأغراض تدريب الموظفين، يُرجى التواصل مع قسم تقنية المعلومات.

3.6. الاستخدام غير القانوني:

لا يجوز للموظفين استخدام الإنترنت عن علمٍ لأغراضٍ تُخالف القوانين التركية. كما لا يجوز لهم استخدام الإنترنت للبحث عن موادّ أو تنزيلها أو الوصول إليها أو البحث عنها بأيّ شكلٍ من الأشكال، ممّا قد يُسيء إلى الموظفين الآخرين أو يُميّز ضدّهم على أساس الجنس أو العرق أو المعتقد الديني أو الميول الجنسية أو الإعاقة أو أيّ أسبابٍ أخرى.

3.7. التسوق عبر الإنترنت:

قد يُسمح للموظفين بإجراء عمليات شراء عبر الإنترنت خلال ساعات العمل الممتدة. مع ذلك، من المهم التذكير بأنه لا يجوز تثبيت برامج البائع على جهاز الكمبيوتر أو أي أجهزة أخرى. على الرغم من أن معايير الأمان في الشبكة المُقدمة لا تقل عن معايير الشبكات المستخدمة في المنازل، إلا أن شركتنا غير مسؤولة عن أمان المعاملات المالية. يجب ألا تتضمن المشتريات مطلقًا أي مواد "فاحشة أو إباحية أو تنتهك الخصوصية"، بالإضافة إلى المواد المصنفة ضمن فئة الأنشطة المحظورة.

3.8. الأمن:

بصفتكم موظفين مسؤولين عن الوصول إلى الشبكة وأمنها، من الضروري عدم مشاركة اسم المستخدم وكلمة المرور مع أي شخص. في هذا السياق، يجب قفل أجهزة الكمبيوتر عند عدم استخدامها بالضغط على Ctrl+Alt+L أو Ctrl+Alt+Del. في حال فقدان أو سرقة أي من الأجهزة الشخصية المستخدمة للوصول إلى بريد الشركة الإلكتروني أو بياناتها، يجب إبلاغ قسم تقنية المعلومات فورًا. كما يجب على موظفينا الإلمام بسياسة أمن المعلومات، التي تتضمن معلومات تفصيلية حول حماية كلمات المرور وأمنها.

3.9. الأنشطة المحظورة:

تشمل الأنشطة المحظورة على الإنترنت الأدوات التالية:
يشمل ذلك مراقبة المنتج وتخزينه وتوزيعه أو استخدامه بأي شكل آخر.

- الأنشطة غير القانونية (بما في ذلك جميع أشكال انتهاك حقوق النشر)
- السلوك التهديدي أو المسيء أو المضايق أو التمييزي
- أشكال التشهير والتحريض على القذف
- الرسائل الفاحشة أو الاستفزازية أو الخاصة، أو الصور المزعجة، أو المواد الإباحية
- أي شيء قد يلحق الضرر بشركتنا في حال عدم الحصول على إذن مسبق

أنشطة

•الرسائل المتسلسلة المرسلة عبر البريد الإلكتروني •الأنشطة الفردية أو التجارية التي تُجرى
لتحقيق الربح •الأعمال الخبيثة والضارة •الاستخدامات السياسية أو الدينية أو الترفيهية غير اللائقة.

3.10. الالتزام بالحماية:

يجب على أي موظف يصادف عن طريق الخطأ صوراً تحتوي على إساءة معاملة الأطفال أثناء استخدام شبكة الشركة أن يبلغ قسم تكنولوجيا المعلومات على الفور عن مكان وجود الصور، ويجب ألا يقوم بنسخ هذه الصور أو توزيعها على أي شخص.

3.11. اعتبارات الأمن والوصول:

3.11.1. اتخذت الشركة تدابير لحماية نفسها وأنظمة حاسوبها ومواقعها الإلكترونية وموظفيها من التهديدات الأمنية الخارجية والداخلية الحالية والمحتملة. تشمل هذه التدابير الأمنية، على سبيل المثال لا الحصر، ما يلي: جدران الحماية وخوادم البروكسي المستخدمة لحظر حركة مرور الإنترنت الواردة والصادرة؛ وبرامج مكافحة الفيروسات؛ وبرامج التحكم في الوصول (التي تحظر الوصول إلى مواقع إلكترونية محددة)؛ وتدابير لمنع تثبيت البرامج؛ وبرامج تقيّد البرامج النصية والعناصر التي قد تكون ضارة.

3.11.2. تتلقى الشركة خدمات تصفية من خادم الإنترنت الخاص بها. وبينما لا تقوم الشركة بحظر الوصول إلى الإنترنت لموظفيها الذين يستخدمون شبكتها، فقد تحظر الوصول إلى المواقع التي تحتوي، أو يُشتبه في احتوائها، على محتوى غير قانوني أو إباحي أو غيره من المحتويات المزعجة (مثل الرسائل الجنسية الصريحة، والدردشة عبر الإنترنت، والأنشطة الإجرامية، والمخدرات، والكحول والتبغ، والمقامرة والألعاب، ومواقع التعارف والصداقة، وأخبار يوزنت، والعنف والأسلحة، وما إلى ذلك).

3.11.3. يجب أن يكون مستخدمو الإنترنت على دراية بأن العديد من مواقع الويب تقوم أحيانًا بتسجيل تفاصيل استخدام الموقع سرًا وأن الوصول إلى الإنترنت والنشاط يترك سجلًا على جهاز الكمبيوتر الخاص بهم.

3.11.4. تحتفظ الشركة بالحق في قطع الوصول إلى الإنترنت دون إشعار مسبق إذا اشتبهت في حدوث خرق أمني يتطلب إجراءً فوريًا أو إذا رأت أن شبكة الشركة و/أو أنظمة الكمبيوتر الخاصة بها معرضة للخطر.

4. سياسة وإرشادات البريد الإلكتروني

4.1. الغرض من هذه السياسة هو ضمان الاستخدام السليم لأنظمة البريد الإلكتروني.
يلتزم كل موظف مُصرَّح له بالوصول إلى خدمة البريد الإلكتروني بالامتثال لأحكام هذه السياسة، وضمان استخدام نظام البريد الإلكتروني بمسؤولية وفعالية، وللأغراض المعتمدة فقط. تهدف هذه السياسة إلى توفير معلومات تُرشد الموظفين، لا سيما فيما يتعلق بالتواصل الداخلي للشركة عبر البريد الإلكتروني. على سبيل المثال، يُحظر استخدام نظام البريد الإلكتروني الخاص بالشركة لأغراض شخصية.

4.2. حالة مراسلات البريد الإلكتروني:

يجب على موظفينا أن يضعوا في اعتبارهم دائمًا أن مراسلات البريد الإلكتروني تُعدّ وثيقة قابلة للكشف عنها في الإجراءات القانونية. جميع رسائل البريد الإلكتروني المُرسلة أو المُستلمة على شبكة البريد الإلكتروني الخاصة بشركتنا هي ملك للشركة، ولا يحق للمستخدمين توقع أي خصوصية شخصية عند استخدام نظام البريد الإلكتروني. يحق لقسم تقنية المعلومات مراقبة رسائل البريد الإلكتروني وسجلات الشبكة لضمان الامتثال لسياسات الشركة. يُعتبر جميع المستخدمين موافقين على هذه المراقبة والمراجعة لرسائل البريد الإلكتروني.

4.3. رسائل البريد الإلكتروني الشخصية:

يُسمح لمستخدمي نظام البريد الإلكتروني بإرسال واستقبال الرسائل الشخصية الداخلية والخارجية. مع ذلك، يجب ألا يتعارض هذا الاستخدام مع عمل المستخدم أو عمل مستخدم آخر، أو يُخلّ بواجباته ومسؤولياته. ينبغي تجنب الإفراط في استخدام البريد الإلكتروني للأمور الشخصية. لا يجوز استخدام نظام البريد الإلكتروني لأغراض تجارية خاصة أو للكشف عن المعلومات السرية الخاصة بالشركة أو توزيعها أو نشرها بأي شكل من الأشكال.

4.4. المحتوى:

يجب أن تخلو جميع رسائل البريد الإلكتروني، سواء كانت صريحة أو ضمنية، من الإشارات الجنسية أو العنصرية أو الدينية أو الجرائم أو التحرش، ويجب كتابتها باستخدام لغة مقبولة فقط للتواصل المهني في مكان العمل.

4.5. الخصوصية:

لا يُمكن ضمان سرية رسائل البريد الإلكتروني. قد يطلع زملاء آخرون غير المُستلم على أي رسالة مُرسلة أو مُستلمة، سواءً عن طريق الخطأ (كترك نافذة مفتوحة مثلاً) أو عن قصد (كأن يحتاج المُستلم لفتح بريد إلكتروني لتشخيص مشاكل الاتصال). لذا، لا يُمكن اعتبار الرسائل خاصة أو سرية. يجب كتابة الرسائل الشخصية مع مراعاة إمكانية اطلاع جهات خارجية على محتواها. أما رسائل البريد الإلكتروني الخارجية، فهي بطبيعتها غير آمنة، وقد يتم اعتراضها وقراءتها من قِبل جهات خارجية دون علمنا. يجب إرسال الرسائل ذات مستوى مُعين من السرية أو الحساسية عبر وسيلة بديلة، وباستخدام الطرق المُحددة في سياسة أمن المعلومات وأمن نقل البيانات.

4.6. مرفقات الملفات:

للحيلولة دون نسخ أي مواد غير لائقة إلى شبكة الشركة، وللحد من خطر الإصابة بالفيروسات، لا يُسمح بتنزيل الملفات المرفقة (صور، نصوص، أو جداول بيانات) في رسائل البريد الإلكتروني إلا إذا كانت من مصادر موثوقة -أي من جهات اتصال معروفة الهوية -ولا تحتوي على محتوى غير لائق. يُرجى عدم فتح ملفات البرامج التنفيذية المرفقة برسائل البريد الإلكتروني، بل يجب إعادة توجيه هذه الرسائل إلى مدير تقنية المعلومات للحصول على المشورة. تشمل امتدادات الملفات التنفيذية: .EXE، .MOC، game.exe، .SCR، .VBSو screen.scr.

4.7. الرسائل المتسلسلة/النكات:

تُعدّ الرسائل المتسلسلة والمراسلات الفكاهية استخدامًا غير لائق لوقت موظفي الشركة ومواردها، وقد تُسيء إلى المُستلم دون قصد. لذا، يجب عدم إعادة توجيه هذه الرسائل إلى مستخدمين آخرين، وحذفها من الشبكة فور وصولها إلى صندوق الوارد.

4.8. تحذيرات خاطئة بشأن الفيروسات:

لا ينبغي إعادة توجيه الرسائل الواردة من جهات خارجية والتي تحتوي على تحذيرات من الفيروسات إلى مستخدمين آخرين. في الواقع، معظم هذه الرسائل لا أساس لها من الصحة. ومع ذلك، في جميع الأحوال، يجب حذفها من صندوق الوارد بعد التواصل مع فريق الدعم الفني والحصول على نصيحتهم.

4.9. استخدام أنظمة البريد الإلكتروني الخارجية لإجراء معاملات الشركة:

يجب إرسال جميع المراسلات الإلكترونية المتعلقة بأعمال الشركة ومعاملاتها عبر شبكة البريد الإلكتروني الخاصة بها. يُحظر استخدام أنظمة وحسابات البريد الإلكتروني الشخصية (مثل Hotmailو AOLوخدمات البريد الإلكتروني التي يقدمها مزودو خدمة الإنترنت، وغيرها من خدمات البريد الإلكتروني غير المذكورة هنا) لأغراض العمل. على الموظفين الذين يحتاجون إلى الوصول إلى شبكة الشركة من خارج مبنى الشركة التواصل مع فريق دعم الهوية للحصول على المشورة بشأن العمل عن بُعد.

4.10. إرشادات إرسال رسائل البريد الإلكتروني:

4.10.1. تحديد مستلمي البريد الإلكتروني:

أ) التحقق بعناية: لتجنب أخطاء إرسال البريد الإلكتروني الشائعة، مثل الاستخدام غير الصحيح لأيقونات "الرد على الكل" و"الرد"، يجب التحقق بعناية من عناوين المستلمين قبل إرسال رسائل البريد الإلكتروني.

ب) المُستلِم الرئيسي: بالإضافة إلى إدخال اسم المُستلِم الرئيسي في خانة العنوان في رأس البريد الإلكتروني، يجب أن يكون عنوان الرسالة "رسالة إلى "xxxxأو "عزيزي/عزيزتي/سيدي/سيدتي "xxxxلتوضيح هوية المُستلِم والجهة المُتوقع منها الرد. يجب إرسال نسخة إلى المُستلِمين لأغراض إعلامية فقط. عند إرسال بريد إلكتروني، يجب إدخال خانة "نسخة إلى".

الشخص الذي تُضيفه إلى خانة "نسخة إلى" هو شخص ترغب في إبلاغه بالموضوع، حتى لو لم يكن هو المُستلم المُباشر للبريد الإلكتروني. عند إضافة شخص إلى هذه الخانة، سيظهر ذلك لجميع مُستلمي البريد الإلكتروني. بعبارة أخرى، بإضافة شخص إلى هذه الخانة، فأنت تُشير ضمنيًا إلى أنه سيكون على علم بالبريد الإلكتروني.

ج) قوائم النسخ الكربونية: كما ينبغي على كل مستخدم أن يُولي اهتمامًا دقيقًا لقائمة المُستلمين وقائمة النسخ في أي رسالة أو مذكرة، ينبغي توخي الحذر نفسه عند كتابة الرسائل الإلكترونية. وعلى وجه الخصوص، يجب تجنب استخدام قوائم نسخ كربونية متعددة في الرسالة الإلكترونية. ينبغي إجراء تحليل دقيق لتحديد ما إذا كان هناك غرض حقيقي وفعّال لنسخ المعلومات أو طلب رأي كل شخص تُنسخ معلوماته. لا ينبغي استخدام قوائم النسخ الكربونية في الرسائل الإلكترونية المُرسلة إلى مجموعات العملاء؛ بل يجب إرسال هذه المراسلات عبر البوابة الإلكترونية. يجب توخي الحذر الشديد لتجنب استخدام قوائم عناوين البريد الإلكتروني في خانتي "إلى" أو "نسخة كربونية" احترامًا لخصوصية المُستلم.

د) قوائم النسخة المخفية :(BCC)تشير "BCC"إلى النسخة المخفية. سيتلقى عنوان البريد الإلكتروني المُدخل في هذا الحقل الرسالة المقصودة. لا يمكن للمستلمين في حقلي "إلى" و"نسخة" رؤية عناوين البريد الإلكتروني المُدخلة في هذا الحقل. فقط المُرسِل والمستلم الذي تم إدخال عنوان بريده الإلكتروني في هذا الحقل يمكنهما رؤية هذه المعلومات. مع ذلك، يمكن لمن تم إدخال أسمائهم في حقل "النسخة المخفية" رؤية هوية المستلمين في حقلي "إلى" و"نسخة".

على الرغم من أن خاصية "الترجمة المخفية" (BCC)قد تكون مناسبة في رسائل البريد الإلكتروني المرسلة إلى أطراف ثالثة، إلا أن حجب المعلومات السرية عن طرف أو أكثر في المراسلات المهنية قد يكون فكرة سيئة، لأن رسائل البريد الإلكتروني قد تُعاد توجيهها لاحقًا، مما قد يكشف معلومات كان من المفترض الحفاظ على سريتها. وقد تنشأ مشاكل تتعلق بالثقة عندما تُشارك رسائل يعتبرها البعض خاصة بهذه الطريقة، ولذلك، يُنصح عمومًا بتجنب استخدام خاصية "الترجمة المخفية" بين الزملاء.

هـ) رسائل البريد الإلكتروني الجماعية: يجب استخدام خدمة إرسال البريد الإلكتروني الجماعي لأغراض العمل الخاصة بالشركة فقط. ولا يجوز استخدامها لإرسال رسائل فردية تحت أي ظرف من الظروف.
بالإضافة إلى ذلك، فإن الترويج أو التوصية بسلع وخدمات أطراف ثالثة أمر غير لائق أيضاً.

و) إرسال مرفقات المستندات/جداول البيانات: يمكن استخدام البريد الإلكتروني لتوزيع ملاحظات التذكير أو مرفقات المستندات الأخرى. مع ذلك، لا يُنصح بإرسال الملفات والمرفقات التي يزيد حجمها عن 10ميجابايت عبر البريد الإلكتروني. يمكن لفريق دعم تقنية المعلومات تقديم المشورة بشأن إرسال الملفات الكبيرة باستخدام وسائل أخرى مثل التخزين المشترك.

.5حماية البيانات الشخصية:

أي مراسلات تتضمن بيانات شخصية تخضع لقوانين حماية البيانات المعمول بها. سياسة شركتنا لمعالجة وحماية البيانات الشخصية و...

تحتوي سياسة أمن المعلومات على معلومات مفصلة حول كيفية الحفاظ على أمان البيانات الشخصية، وينبغي أن يكون كل موظف على دراية بها.