Machine Translated by Google

الاتصالات الإلكترونية و البيانات الإلكترونية حول عملية التفتيش أنظمة

IKVKK_Y4الإصدار 1.00

Machine Translated by Google

.1الغرض والنطاق

.1.1الغرض من هذه اللائحة هو تحديد الإجراءات والمبادئ المتعلقة بشروط وتوقيت مراقبة الشركة للاتصالات الإلكترونية، وتسري أحكام هذه اللائحة على الموظفين والأطراف الثالثة المصرح لهم بالوصول إلى و/أو استخدام مرافق الاتصالات الإلكترونية الخاصة بالشركة.

.2مراقبة الاتصالات الإلكترونية

.2.1لأغراض هذه اللائحة، تشير الاتصالات الإلكترونية عمومًا إلى جميع أنواع الرسائل الإلكترونية، بما في ذلك المكالمات الهاتفية، ورسائل الفاكس، ورسائل البريد الإلكتروني، والرسائل الفورية، والرسائل النصية القصيرة (SMS)أو غيرها من الرسائل القصيرة، والتغريدات، ومواقع الويكي، والمدونات، ومحتوى الويب المنشور على منصات المراسلة. لا تتحمل الشركة أي مسؤولية أو واجب لمراقبة محتوى الاتصالات الإلكترونية لموظفيها أو زوارها بشكل عام نظرًا لطبيعة عملياتها. علاوة على ذلك، لا تُجري الشركة فحصًا عامًا للاتصالات الإلكترونية بشكل روتيني من خلال أخذ عينات عشوائية أو تدخل بشري. ومع ذلك، يتم إجراء فحص آلي بمساعدة الحاسوب لحركة البريد الإلكتروني على نطاق محدود لمنع رسائل البريد الإلكتروني الجماعية غير المرغوب فيها (المعروفة باسم "البريد العشوائي") ومحتوى الرسائل الذي قد يكون ضارًا (فيروسات الحاسوب، ومحاولات الاحتيال المالي، وما إلى ذلك).

.2.2.5.4يُقرّ جميع المستخدمين بأنه باستخدام أنظمة الاتصالات الإلكترونية التي توفرها الشركة، لا تُقدّم الشركة أي ضمانات بشأن سرية أي رسائل أو بيانات مُخزّنة على هذه الأنظمة أو مُرسلة من خلالها؛ وأن الشركة تحتفظ بحقوقها كما هو مُبيّن في هذه الوثيقة؛ وأن استخدام هذه الأنظمة يقتصر على الأغراض التي تُقرّها الشركة، وأنهم قد أُبلغوا بذلك. إن استخدام أنظمة الاتصالات الإلكترونية الخاصة بالشركة فيما يتعلق بأنشطة الشركة والاستخدام الشخصي غير الضروري ليس حقًا، بل هو امتياز ممنوح لموظفيها وللأطراف الثالثة المُصرّح لها.

لذلك، يجوز للشركة، في أي وقت ودون إشعار مسبق، حجب الوصول كليًا أو جزئيًا إلى جميع أو جزء من أنظمة الاتصالات الإلكترونية وأنظمة تكنولوجيا المعلومات الخاصة بها (لجميع المستخدمين أو بعضهم). يلتزم مستخدمو أنظمة الاتصالات الإلكترونية وأنظمة الحاسوب التابعة للشركة بالامتثال للائحة الشركة بشأن الإجراءات والمبادئ المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات، وللقسم 11.9 "شروط الاستخدام المقبول لموارد تكنولوجيا المعلومات (سياسة الاستخدام المقبول)" من سياسة أمن المعلومات. وباستخدام هذه الأنظمة، يُقرّ المستخدمون بقبولهم لسياسة الاستخدام المقبول والتزامهم بها، وبأنهم قد أُبلغوا بها، وبموافقتهم على تطبيق الشركة لها. كما يوافق المستخدمون على الامتثال للتشريعات ذات الصلة والامتناع عن أي سلوك يُلزم الشركة. ويجوز للشركة، في أي وقت ودون إشعار مسبق، تغيير لائحة الإجراءات والمبادئ المتعلقة بالاستخدام الأمثل للإنترنت وأدوات الاتصالات الإلكترونية، وغيرها من الشروط المتعلقة باستخدام أنظمة الحاسوب.

Machine Translated by Google

نحتفظ بالحق في إجراء تغييرات واتخاذ أي إجراء مطلوب أو مناسب بموجب التشريعات ذات الصلة.

2.3. وفقًا للمادة 6 من القانون رقم 5651 بشأن 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 المنصوص عليها في القانون، ولضمان دقة هذه المعلومات وسلامتها وسريتها. وتشمل هذه التدابير، 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 مثل الفيروسات والاختراق وهجمات حجب الخدمة، وضمان امتثال عمليات تقنية المعلومات لسياسات الشركة وتوجيهاتها.

2.4. تتم مراقبة الاتصالات الإلكترونية في المقام الأول بموافقة الشخص المعني. ومع ذلك، تحتفظ الشركة بحقها في إجراء المراقبة من تلقاء نفسها لتحقيق أغراضها المشروعة في الحالات التالية:

2.4.1. الاحتفاظ بسجلات المعاملات والاتصالات الأخرى حيث يكون من الضروري أو المرغوب فيه معرفة عناصر معينة من الاتصال بين الأطراف المعنية من أجل ضمان أمن الأعمال والمعاملات المالية والاقتصادية؛

2.4.2. للتأكد من الامتثال للوائح والممارسات المتعلقة بالشركة، مثل التحقق مما إذا كانت اللوائح الإدارية للشركة والمبادئ التوجيهية الداخلية وقواعد السلوك قيد التنفيذ؛

2.4.3. تحديد أو إثبات المعايير التي يجب على الأشخاص الذين يستخدمون أنظمة المعلومات الإلكترونية للشركة تحقيقها لأغراض مثل مراقبة الجودة أو تدريب الموظفين؛

2.4.4. المراقبة أو التسجيل لمنع أو اكتشاف الأعمال الإجرامية، على سبيل المثال الفساد أو إساءة استخدام أنظمة الكمبيوتر أو غيرها من الأنشطة غير القانونية.

2.4.5. لمنع أو اكتشاف الاستخدام غير المصرح به لأنظمة المعلومات والاتصالات الإلكترونية، على سبيل المثال، لمنع الموظفين من انتهاك لوائح الشركة المذكورة في القسم 11: "شروط استخدام موارد تكنولوجيا المعلومات (سياسة الاستخدام المقبول)" من سياسة أمن المعلومات؛

2.4.6. لضمان التشغيل الفعال للنظام عن طريق اكتشاف الفيروسات وإزالتها، والتحكم في التهديدات الأخرى للنظام وإيقافها مثل الاختراق أو هجمات حجب الخدمة؛ وعن طريق إنشاء تدفقات الشبكة وسجلات البريد الإلكتروني؛

2.5. يجب على الأفراد الذين يستخدمون أنظمة الاتصالات الإلكترونية للشركة أن يدركوا أن مسؤولي أنظمة وشبكات تكنولوجيا المعلومات والاتصالات يراقبون عمليات الإرسال أو يطلعون على معلومات المعاملات بشكل دوري لضمان حسن سير خدمات تكنولوجيا المعلومات في الشركة. في مثل هذه الحالات، قد يصل الموظفون المعنيون عن غير قصد إلى معلومات إلكترونية.

Machine Translated by Google

قد يكونون على دراية بمحتوى المراسلات. ما لم يُنص على خلاف ذلك في هذه اللائحة أو التشريعات ذات الصلة، يُحظر على المسؤولين المذكورين أعلاه الاطلاع عن علم على محتوى معلومات معاملات موظفي الشركة أو استخدام ما شاهدوه أو سمعوه أو قرأوه بأي شكل من الأشكال. مع ذلك، في حال اكتشاف أي انتهاك لسياسات الشركة أو لوائحها الإدارية أو أحكامها القانونية، يجب إبلاغ السلطات العليا في الشركة بذلك.

3.تحليل البيانات الإلكترونية

3.1.قد تحتاج الشركة من حين لآخر إلى مراجعة رسائل البريد الإلكتروني الخاصة بالشركة والمخزنة على أجهزة تخزين متصلة بالشبكة أو مستقلة، والمستندات والملفات الموجودة على محركات الأقراص المحلية أو الرئيسية أو الجماعية، والبيانات المتعلقة بسجلات الوصول إلى أنظمة الشركة أو مبانيها. إضافةً إلى ذلك، يُعتبر الموظفون والزوار الذين يتصلون بشبكة الشركة بأجهزتهم الشخصية موافقين على مراقبة بياناتهم للأغراض المحددة في القسم 6من سياسة أمن المعلومات الخاصة بالشركة، بعنوان "مراقبة الاتصالات الإلكترونية". تقتصر عمليات التدقيق هذه على ضمان أمن البيانات، وستُجرى وفقًا للمبادئ المنصوص عليها في القانون رقم 6698بشأن حماية البيانات الشخصية.

3.2.في الظروف العادية، ستحصل الشركة على موافقة المستخدم قبل إجراء أي مراجعة للبيانات التي يحتفظ بها الأفراد أو المتعلقة بهم، مثل حسابات البريد الإلكتروني، والسائقين الرئيسيين أو المحليين، وسجلات الوصول. ومع ذلك، ستُجرى المراجعة حتى في حال عدم منح المستخدم الإذن في الحالات التالية:

3.2.1.حيثما ينص القانون على ذلك؛

3.2.2.إذا كانت هناك أدلة موثوقة تتجاوز مجرد الثرثرة أو الشائعات، وكان هناك شك قوي في أن الأحكام القانونية أو سياسات الشركة قد تم انتهاكها؛

3.2.3.في الظروف القاهرة والحالات الطارئة التي قد يؤدي فيها عدم التصرف إلى ضرر جسدي خطير، أو خسارة كبيرة أو تلف في الممتلكات، أو فقدان أدلة مهمة على انتهاك القانون أو سياسات الشركة ولوائحها، أو التزامات مالية كبيرة على الشركة أو موظفيها و/أو مديريها؛

3.2.4.قد يؤثر عدم اتخاذ إجراء على الأداء الإداري أو المالي للشركة.
إذا كان من المحتمل أن تتأثر قدرتهم على الوفاء بمسؤولياتهم بشدة.

3.3.إذا كان المستخدم المعني موجودًا خارج مباني الشركة ومرافقها، وكان فحص البيانات التي يحتفظ بها أو المتعلقة به ضروريًا لأسباب تجارية، فيجب الحصول على موافقته أولًا. وفي حال تعذر التواصل معه، يجوز لرئيس القسم المعني والمدير العام منح إذن كتابي لإجراء تدقيق على الحاسوب أو الأجهزة الأخرى المخصصة له لأغراض تسيير أعمال الشركة. وفي هذه الحالة، يجب الحصول على الموافقة اللازمة.

Machine Translated by Google

سيتم تسجيل الإجراءات والأسباب التي تستدعي إجراء عمليات التفتيش في تقرير.

3.4.إذا كان من الضروري مراجعة البيانات التي يحتفظ بها المستخدم أو البيانات المتعلقة بالأفراد، كما هو مذكور في القسم 3.2أعلاه، دون الحصول على موافقة صاحب البيانات، فسيتم تطبيق القواعد التالية:

3.4.1.حالات الطوارئ: يجوز فحص الحد الأدنى من متطلبات حالة الطوارئ، ويجوز اتخاذ الحد الأدنى من التدابير اللازمة لمعالجة الوضع على الفور دون إذن؛ ومع ذلك، بمجرد انتهاء حالة الطوارئ، يجب طلب الإذن المناسب دون تأخير، ويجب تسجيل الحالة وفقًا للفقرة 3.3؛

3.4.2.في جميع الحالات الأخرى، لن يتم اتخاذ أي إجراء دون الحصول على إذن كتابي من رئيس القسم المعني والمدير العام.

3.4.3.البيانات المشفرة: إذا تم العثور على بيانات مشفرة أثناء تدقيق النظام، فيجب تقديم مفتاح فك التشفير عند الطلب.

3.4.4.تعود ملكية البيانات التي أنشأها أو تتعلق بالموظفين الذين لم يعودوا يعملون لدى شركتنا إلى الشركة، وذلك وفقًا لأحكام فترات الإتلاف القانونية. ولا يلزم الحصول على إذن من الموظف المنتهي خدمته للاطلاع على هذه المعلومات. ويجب الحصول على إذن الاطلاع على المعلومات باتباع الإجراءات المحددة في البند 3.3أعلاه.

3.5.بمجرد منح الإذن، ستتم معالجة البيانات الموجودة في أنظمة الشركة على النحو التالي:
سيتم مناقشة ما يلي:

3.5.1.سيتم تقييم المواد المتعلقة بالشركة وفقًا لممارسات العمل العادية.
سيتم الاحتفاظ بها أو حذفها حسب الضرورة.

3.5.2.لن يتم فحص البيانات الشخصية إلا إذا كان هناك سبب مشروع.

3.5.3.يتحمل موظفو الشركة مسؤولية حذف بياناتهم الشخصية الموجودة في المستندات الإلكترونية ورسائل البريد الإلكتروني قبل إنهاء خدمتهم.

3.6.الخصوصية: تُجرى جميع عمليات التدقيق بموجب هذه اللائحة مع مراعاة تامة لحق الخصوصية. تخضع المواد المتعلقة بالحياة الخاصة للأفراد للحد الأدنى من التدقيق اللازم لأغراض التدقيق. أي معلومات سرية يتم العثور عليها ولا صلة لها بغرض البحث لن تُفصح لأي طرف وستبقى سرية. مع ذلك، إذا عُثر أثناء عمليات التدقيق على أي مواد غير قانونية أو مخالفة لسياسات الشركة، يُبلّغ المدير العام فورًا، ويُتخذ الإجراء اللازم وفقًا لتوجيهاته.