



# سياسة وإجراءات تسرب المعلومات تكنولوجيا المعلومات لشركة بهتكو القابضة



الغرض يسعى قسم تكنولوجيا المعلومات إلى حماية البيئة من تهديدات أمن المعلومات التي قد تؤثر على الخصوصية والإنتاج والسمعة وحقوق الملكية الفكرية، ولذلك فقد تم تطوير هذه الوثيقة. لتلخيص مجموعة من السياسات والإجراءات التي تحكم عملية المراقبة الأمنية في قسم تكنولوجيا المعلومات، نطاق تطبيق هذه السياسة والإجراءات المرتبطة بها ضمن صلاحيات إدارة تقنية المعلومات تحت الإشراف المباشر لنائب رئيس مجلس الإدارة. ويجب مراعاة الوحدات المختصة أثناء التنفيذ، وهي من أقسام شركة بهتكو القابضة لإدارة الاستثمار.



تعريف مستخدم بنية تحتية بروتوكولات الجدار الحماية  
ووحدات تجارية  
المصطلحات والتعاريف  
أي موظف يستخدم نظام تكنولوجيا المعلومات لشركة  
باهتكو القابضة لإدارة الأصول مسؤول عن تقديم كافة  
خدمات تكنولوجيا المعلومات من خلال الأجهزة  
الأساسية.

.



ARP.

LAN

تكون المعلومات عنوان الملكية الفكرية. مجموعة البنية التحتية في إدارة تكنولوجيا المعلومات.

حركة المرور، والمعروفة أيضًا باسم منع الهجمات، هي جزء من نظام كمبيوتر أو شبكة كمبيوتر مصممة لمنع الوصول غير المصرح به مع السماح بالاتصال الخارجي.

هذا البروتوكول قد يسمح للمهاجمين بالحصول على إطارات البيانات على الشبكة وتعديل حركة المرور أو إيقافها



## الغنم

الوكيل خادم يعمل كوسيط بين مستخدم محطة العمل  
والإنترنت.

شركة بهتكو القايزة وشركائها التابعة. مزود خدمة  
الإنترنت.

مجموعة الدعم الفني بقسم تكنولوجيا المعلومات.



## معييار

المسؤوليات يتحمل المستخدمون مسؤولية استخدام الوصول إلى الإنترنت بطريقة احترافية والحصول على معرفة عملية بتعليمات تشغيل.

وحدة تقوم بدمج جميع عناصر الشبكة في نفس الشبكة.  
الإنترنت

إساءة استخدام أنظمة المراسلة الإلكترونية بما في ذلك وسائل البث وأنظمة التسليم الرقمية لإرسال الرسائل. هوية رقمية وعنوان منطقي مخصص للأجهزة التي تشارك في شبكة الكمبيوتر.



آمنة لجميع المستخدمين. الدعم الفني هو المسؤول عن نقل أو توصيل أجهزة الكمبيوتر إلى شبكة الشركة. تقديم خدماتها بطريقة فعالة وآمنة للوحدات ذات الصلة. مجموعة البنية التحتية مسؤولة عن مراقبة الإنترنت وسجلات جدار الحماية وإدارة امتيازات الوصول لتوفير بيئة آمنة.

يتحمل المستخدمون مسؤولية الالتزام بجميع السياسات التي تمت صياغتها والإعلان عنها من قبل قسم تكنولوجيا المعلومات المتعلقة بمجموعة تقنية المعلومات، المسؤولة عن تأمين البنية التحتية لشركة بهتكو القايزة وشركاتها التابعة.



دليل سياسة الخدمة. إنه موجود في دليل سياسة  
الخدمة.

إزالة امتيازات الوصول إلى الإنترنت لا يسمح  
للمستخدمين بنقل أو توصيل أي أجهزة تكنولوجيا  
المعلومات، بما في ذلك أجهزة الكمبيوتر والهواتف، مع  
بروتوكول الطابعات.

سيتم حجب خدمات الإنترنت دون إشعار مسبق لأي  
مستخدم ينتهك السياسات المتعلقة بالإنترنت، كما هو  
مذكور سابقًا. سيتم حظر الوصول إلى المواقع غير  
المرغوب فيها، سواء كانت إلكترونية أو غيرها، من  
مصادر مشبوهة بواسطة مزود خدمة الإنترنت. سيتم  
أيضًا حظر رسائل البريد الإلكتروني الاحتيالية لضمان أمان  
البريد الإلكتروني لشركتك.

تحفظ إدارة تقنية المعلومات الحق في حجب المواقع غير  
المرغوب فيها دون إشعار مسبق بناءً على تصنيف  
المواقع المذكورة.



دون التنسيق مع قسم تكنولوجيا المعلومات.

يجب على الشبكة اتخاذ الخطوات اللازمة لتمكين جهاز المستخدم من  
الاتصال بالشبكة.

يتم استخدام منفذ الشبكة المعتمد لتعيين جميع أجهزة المستخدم  
(أجهزة الكمبيوتر والهواتف) بروتوكول مخصص للواجهة المحددة في  
المحول.



## شركة

إجراءات لدى مجموعة إدارة البنية التحتية وتكنولوجيا المعلومات تتضمن العديد من انتهاكات خدمة الإنترنت. سيتم تعزيز أمان الشبكة من خلال منع هجوم الأمان الذي تم تحقيقه من خلال مجموعة البنية التحتية: الإجراءات لضمان سلامة وأمن موارد البنية التحتية، وفيما يلي الاحتياطات:

سيتم إنشاء تقارير شهرية لاستخدام الإنترنت من قبل فريق البنية التحتية فيما يتعلق بالمستخدمين المخالفين مع تفاصيل المخالفة.



من المنفذ ستتم مراجعة التقارير والسجلات الشهرية من  
بوابة مكافحة الاحتيال وجدار الحماية.

حظر رسائل الاحتيال الشائعة واستخدام مجموعة البنية  
التحتية لتتبع أي هجمات وعمليات احتيال.

عند اكتشاف هجمات أو رسائل تصيد تستهدف مواقع  
ضارة، سيتم حظرها بواسطة فريق البنية التحتية لمزود  
الخدمة أو جدار الحماية.

سيتم مراجعة قائمة المستخدمين المخالفين من قبل  
مدير تقنية المعلومات لحظر الخدمة، خلاف ذلك سيتم  
إرسال قائمة المستخدمين المخالفين إلى فريق الدعم  
الفني لاتخاذ الإجراءات اللازمة لحجب خدمة الإنترنت عن  
هؤلاء المستخدمين. سيقوم فريق الدعم الفني بحجب  
المواقع غير المرغوب فيها وإجراء الاختبارات اللازمة  
لتنفيذ الحجب بنجاح من مزود خدمة الإنترنت والوكيل.

يتم إجراء التثبيت اللازم على المفتاح لتمكين توصيل الجهاز.  
يتم إجراء الفحوصات اللازمة للتأكد من نجاح حجب المواقع أو البروتوكولات الدولية. يتم تنفيذ ميزات أمان المنفذ من قبل مجموعة البنية التحتية لمنع المستخدمين من نقل أجهزتهم أو أي جهاز شبكة دون التنسيق مع مجموعة تكنولوجيا المعلومات. لذلك يجب اتخاذ الخطوات التالية عندما تكون هناك حاجة لنقل أجهزة الكمبيوتر أو سيقوم أعضاء مجموعة الدعم الفني بنقل الجهاز إلى الموقع الجديد. يجب على المستخدم في الوحدة إبلاغ فريق الدعم الفني في قسم تكنولوجيا المعلومات لاتخاذ الإجراءات اللازمة لنقل الجهاز.

