سياسة وإجراءات تسرب المعلومات

تكنولوجيا المعلومات

لشركة الدار لإدارة الأصول الاستثمارية "أدام"

adam أدام

الدار لإدارة الأصول الاستثمارية

الغرض

تسعى إدارة تكنولوجيا المعلومات إلى حماية البيئة من تهديدات أمن المعلومات والتي قد تؤثر على الخصوصية والإنتاج والسمعة وحقوق الملكية الفكرية، ومن ثم تم تطوير هذه الوثيقة لتلخيص مجموعة من السياسات والإجراءات الحاكمة لعملية مراقبة الأمن في إدارة تكنولوجيا المعلومات.

المجـــال

يقع مجال تنفيذ هذه السياسة والإجراءات المرتبطة بها ضمن سلطات إدارة تكنولوجيا المعلومات تحت الإشراف المباشر لنائب رئيس مجلس الادارة ومن الضروري الأخذ في الاعتبار الوحدات المختصة خلال التنفيذ والتي تكون من إدارات شركة الدار لإدارة الأصول الاستثمارية.

المصطلحات والتعريفات

المصطلح	التعريف
الوحدة التجارية	شركة الدار لإدارة الأصول الاستثمارات (الإدارات)
المستخدم	أي موظف يستخدم أنظمة تكنولوجيا المعلومات.
البنية التحتية	الأجهزة الأساسية المسئولة عن تقديم جميع خدمات تكنولوجيا المعلومات
الجدار الناري	جزء من النظام الحاسوبي أو الشبكة الكمبيوترية المصممة لمنع الدخول غير المصرح مع السماح بالتواصل الخارجي
بروتوكول تحديد العنوان ARP	قد يسمح هذا البروتوكول للمهاجم بالحصول على إطارات البيانات في شبكة المنطقة المحلية LAN وتعديل المرور أو وقف المرور (والتي تعرف باسم منع الهجوم على الخدمة)
IS	مجموعة البنية التحتية في إدارة تكنولوجيا المعلومات.
TS	مجموعة الدعم الفني في إدارة تكنولوجيا المعلومات.
الشركة	دار الاستثمار والشركات التابعة لها .
ISP	مزود خدمة الإنترنت.
الوكيل	سيرفر يعمل كوسيط فيما بين مستخدم وحدة العمل والإنترنت
الغش	سوء استخدام أنظمة الرسائل الإلكترونية (بما في ذلك وسائط البث وأنظمة التسليم الرقمية) لإرسال الرسائل الكمية غير الموحدة بصورة غير تمييزية
IP	هوية رقمية وعنوان منطقي مخصص للأجهزة التي تشارك في شبكة الحاسوب
المفتاح (سويتش)	جهاز الشبكة الذي يدمج جميع عناصر الشبكة في نفس الشبكة.

المسئوليات

- المستخدمون مسئولون عن استخدام الولوج إلى الإنترنت بطريقة مهنية وأن تكون لديهم معرفة عملية حول تعليمات تشغيل الإنترنت القياسية.
- المستخدمون مسئولون عن الالتزام بجميع السياسات المصاغة والمعلنة من خلال إدارة تكنولوجيا المعلومات.
- إدارة تكنولوجيا المعلومات (مجموعة البنية التحتية) مسئولة عن تأمين البنية التحتية لشركة دار الاستثمار وشركاتها التابعة من أجل تقديم خدماتها بطريقة فعالة ومؤمنة إلى الوحدات المختصة.
- مجموعة البنية التحتية مسئولة عن مراقبة الإنترنت وسجلات الجدار الناري وأمن المنفذ وإدارة امتيازات الولوج المنشورة لتوفير البيئة الآمنة لجميع المستخدمين.
- الدعم الفني مسئول عن نقل أو توصيا الحواسب في شبكة الشركة.

السياسة

- على إدارة تكنولوجيا المعلومات (مجموعة البنية التحتية) إجراء المراقبة الدورية لأي مخالفة لضمان الأمن والسلامة المستمرة لمصادر الشركة وفقاً لسياسات الأمن السارية.
- سواء استخدام امتيازات الولوج إلى الإنترنت والإخفاق في إتباع سياسات الخدمات المنصوص عليها في دليل سياسات الخدمات قد تؤدي إلى إزالة امتيازات الولوج إلى الإنترنت.
- سوف يتم منع خدمات الإنترنت دون إشعار مسبق لأي مستخدم يخالف سياسات الخدمات التي تتعلق بالإنترنت وفقاً لما هو منصوص عليها في دليل سياسات الخدمات.
- تحتفظ إدارة تكنولوجيا المعلومات بالحق في حجب المواقع غير المرغوبة دون إشعار مسبق بناء على تصنيف المواقع المنصوص عليه في دليل سياسات الخدمات.
- سوف يتم حجب المواقع غير المرغوبة / المعدية والمصادر الأخرى المشكوك فيها من جانب ISPs والوكيل.
- سوف يتم حجب رسائل الغش لضمان أمن بريد الشركة الإلكتروني.
- لا يسمح للمستخدمين نقل أو توصيل أي أجهزة تكنولوجيا المعلومات (الحواسب والهواتف المزودة ببروتوكول دولي IP والطابعات وأجهزة ATAs) دون التنسيق مع إدارة تكنولوجيا المعلومات.
- يستخدم أمن منفذ الشبكة لتخصيص كل أجهزة مستخدم (الحواسب والهواتف المزودة ببروتوكول دولي) إلى منفذ معين في مفتاح الشبكة.
- يجب أن تأخذ إدارة تكنولوجيا المعلومات (مجموعة الدعم الفني) الإجراءات اللازمة لتمكين جهاز المستخدم من التوصيل مع شبكة الشركة.
- سوف يتم تعزيز أمن الشبكة من خلال منع هجوم ARP.

الإجراءات

لدى مجموعة البنية التحتية وإدارة تكنولوجيا المعلومات الكثير من الإجراءات لضمان سلامة وأمن مصادر البنية التحتية، وفيما يلي الاحتياطات الأمنية والتي تم تحقيقها من خلال مجموعة البنية التحتية:

مخالفات خدمة الإنترنت:

- يتم إنشاء تقارير استخدام الإنترنت الشهري من خلال فريق البنية التحتية فيما يتعلق بالمستخدمين المخالفين مع تفاصيل المخالفة.
- قائمة المستخدمين المخالفين سوف يتم مراجعتها من قبل مدير تكنولوجيا المعلومات لحجب الخدمة لهذه الخدمة من خلافه.
- ترسل قائمة المستخدمين المخالفين إلى فريق الدعم الفني لأخذ الإجراءات اللازمة لمنع خدمة الإنترنت من هؤلاء المستخدمين.
- سوف تقوم مجموعة الدعم الفني بحجب المواقع غير المرغوبة مع إجراء الاختبارات الضرورية لتنفيذ الحجب بنجاح من جانب ISP والوكيل والجدار الناري.

حجب رسائل الغش الشائعة:

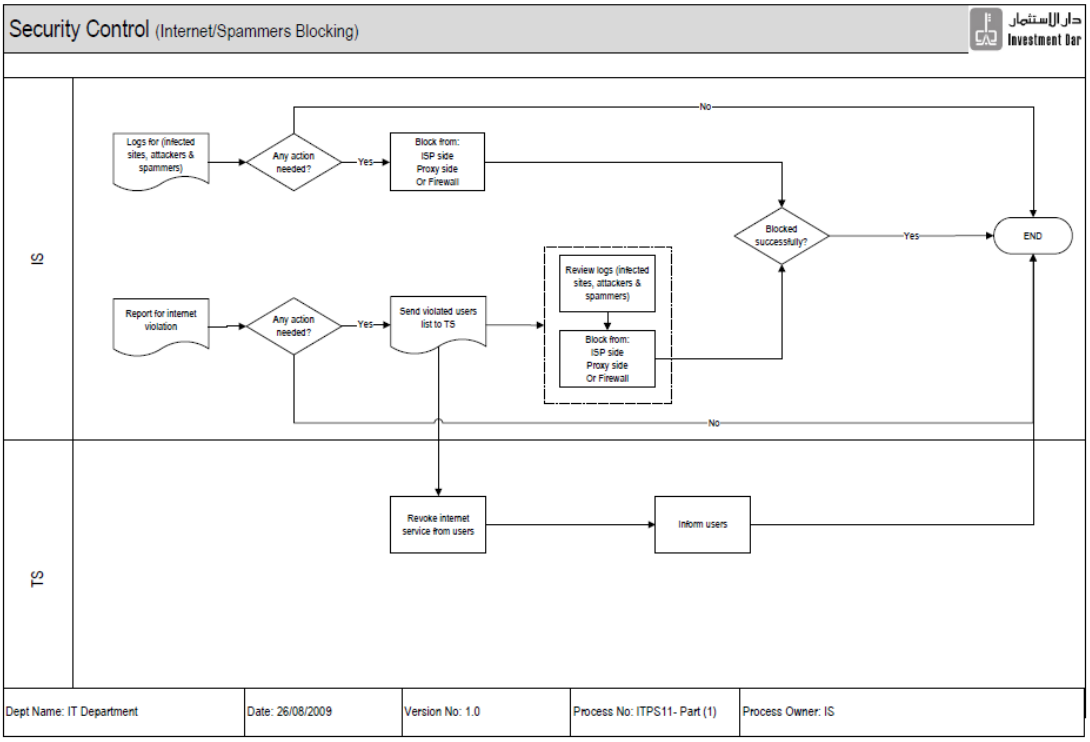
- التقارير الشهرية والسجلات من بوابة مكافحة رسائل الغش والجدار الناري سوف يتم مراجعتها من قبل مجموعة البنية التحتية لتعقب أية هجمات ورسائل غش.
- عند اكتشاف الهجمات ورسائل الغش والمواقع المعدية، سوف يحجبها فريق البنية التحتية من البروكسي أو ISP أو الجدار الناري.
- تجرى الاختبارات الضرورية لضمان إتمام حجب المواقع أو البروتوكولات الدولية بنجاح.

أمن المنفذ:

- تم تنفيذ ميزة أمن المنفذ من خلال مجموعة البنية التحتية لمنع المستخدمين من نقل أجهزتهم أو أية جهاز شبكة دون التنسيق مع مجموعة تكنولوجيا المعلومات المختصة، ومن ثم يجب تحقيق الخطوات التالية عند وجود حاجة إلى نقل أجهزة الحاسوب أو أجهزة الشبكة:
  - على المستخدم (الوحدة) إعلام مجموعة الدعم الفني في إدارة تكنولوجيا المعلومات للقيام بالإجراءات اللازمة لنقل الجهاز.
  - أعضاء مجموعة الدعم الفني سوف ينقلون الجهاز إلى الموقع الجديد.
  - يتم إجراء التنصيب الضروري على المفتاح أو السويتش لتمكين توصيل الجهاز.

العملية:

- **ITPS11 (1):**



- **ITPS11 (2):**