قرار مجلس الإدارة رقم (4) لسنة 2018م

بعد الاطلاع على قانون رقم 15 لسنة 2014 بشأن تنظيم الأعمال الخيرية، وقانون رقم 43 لسنة 2014 بشأن إنشاء هيئة تنظيم الأعمال الخيرية، والتعليمات والتعاميم الصادرة من هيئة تنظيم الأعمال الخيرية، وقرار إنشاء مؤسسة الشيخ عيد الخيرية رقم (36) لسنة 1995م والنظام الأساسي للمؤسسة ودليل الصلاحيات، فإنه وفقاً لما تقتضيه مصلحة المؤسسة، واضطلاع مجلس الإدارة بواجبه في إيجاد بيئة رشيدة محوكمة فقد قرر مجلس الإدارة في جلسته المنعقدة في مقر المؤسسة بتاريخ: 2018/09/18م مايلي:

مادة رقم (1)

اعتماد دليل سياسات أمن المعلومات للعمل به والالتزام بأحكامه من قبل أعضاء مجلس الإدارة وأعضاء اللجان التابعة للمجلس وجميع وحدات ومنتسبي المؤسسة على أساس مبدأ الالتزام أو تفسير عدم الالتزام، وتطبع هذه الوثيقة وتنشر على الموقع الداخلي للمؤسسة لتمكين جميع الأطراف المعنية من الاطلاع عليها.

مادة رقم (2)

يسري العمل بهذا القرار اعتباراً من تاريخ: (01 أكتوبر 2018م) ويلغي كل ما يتعارض معه من قرارات سابقة وعلى جميع الوحدات الإدارية في المؤسسة تنفيذه كل فيما يخصه.

مادة رقم (3)

اســـم الـوثيقـة:	**دليل سياسات أمن المعلومات.**
رقـم الإصدار:	1.0
تاريخ الإصدار:	2018/10/01م
إعداد ومراجعة:	فريق الجودة بإشراف المدير العام.

والله الموفق والهادي إلى سواء السبيل،،،

أعضاء مجلس الإدارة

الشيخ: خليفة بن عيد آل ثاني

الشيخ: عبدالعزيز بن عيد آل ثاني

الشيخ: خالد بن عيد آل ثاني

الشيخ: عبدالله بن عيد آل ثاني

أ.د: علي القره داغي

الشيخ: فيصل بن جاسم آل ثاني

رئيس مجلس الإدارة

الشيخ: محمد بن عيد آل ثاني

إدارة	نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01 - سارية
سياسة	**كلمة المرور**		2017/01/01 -تم مراجعتها
		نظم المعلومات	-المحرر

مقدمة

يُقصد من التحقق من المستخدم هو ضبط الدخول إلى نظام مصدر المعلومات. إن التحكم في الدخول أمر ضروري لأي مصدر معلومات. يمكن أن يتسبب دخول جهة غير مصرح لها في خسارة المعلومات السرية وسلامتها وإتاحتها والذي قد يسبب خسارة الثقة أو التسبب في إحراج لمؤسسة عيد الخيرية.

من الممكن استخدام هذه العوامل أو دمج لهذه العوامل للتحقق من مستخدم. نورد فيما بعد أمثلة على هذا:

- شيء ما تعرفه- كلمة السر، رقم التعريف الشخصي.
- شيء ما لديك- بطاقة ذكية
- شيء ما يميزك- بصمة أصبع
- مجموعة من العوامل – البطاقة الذكية ورقم التعريف الشخصي.

الغرض

تهدف سياسة كلمة المرور لمؤسسة عيد الخيرية تحديد قوانين لإنشاء وتوزيع وحماية وإنهاء وتصحيح آليات التحقق من مستخدم المؤسسة.

الجمهور

تطبق سياسة كلمة المرور لمؤسسة عيد الخيرية على جميع الأفراد المستخدمين لمصدر معلومات عيد الخيرية.

تعاريف

مصادر المعلومات (IR): أي من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

كلمة المرور: سلسلة من الرموز التي تعمل كتحقق من هوية الشخص والتي قد تُستخدم لمنح أو رفض أو الدخول إلى البيانات الخاصة أو المشتركة.

كلمات المرور القوية: كلمة المرور القوية هي كلمة المرور التي يصعب تخمينها. يتم تفسير مجموعة الرموز والأرقام والرموز الخاصة بشكل عام بناء على مدى قدرة نظام التشغيل. وبهذا تكون كلمات المرور الأطول هي الأقوى. يجب ألا تكون اسم أو كلمة في قاموس بأي لغة أو كلمة مركبة أو اسم شائع أو رقم أو كلمة يمكن ربطها مع أي معلومات شخصية عنك مثل تاريخ الميلاد أو رقم التأمين الاجتماعي وهكذا

سياسة كلمة المرور

- قواعد كلمات المرور:
  - ❖ يجب تغييرها دوريًا.
  - ❖ يجب أن تمتثل لأدنى عدد حروف حددتها مصادر المعلومات الخاصة بالمؤسسة.
  - ❖ يجب أن تكون مجموعة من الرموز والحروف والأرقام
  - ❖ ألا تكون سهلة الربط بحساب المستخدم مثل اسم المستخدم أو الرقم الشخصي أو الاسم المستعار أو أسماء الأقارب أو تاريخ الميلاد إلخ.
  - ❖ يجب ألا تكون كلمات في القاموس أو كلمات مركبة.
- يجب تشفير كلمات السر المسجلة
- يجب عدم الإفصاح عن كلمات مرور حساب المستخدم إلى أي شخص.
- في حال التشكك في أمن كلمة مرور، يجب تغييرها فورًا.
- يجب عدم تحايل الإداريين على سياسة كلمة المرور لتسهيل الاستخدام.
- لا يمكن تحايل المستخدمون على دخول كلمة المرور بتسجيل تلقائي أو تذكر الطلب أو نصوص مدمجة أو كلمات مرور بتشفير قوي في برنامج العميل. قد تحدث استثناءات (مثل النسخ الاحتياطي التلقائي) بموافقة موظف أمن المعلومات لدى مؤسسة عيد الخيرية.
- يجب على المستخدم عدم ترك الجهاز مفتوح بدون غلق أو الخروج من الحساب الخاص به.
- يجب أن تتضمن إجراءات تغيير كلمة المرور الإجراءات التالية:
  - ❖ التحقق من المستخدم قبل تغيير كلمة المرور
  - ❖ التغيير إلى كلمة مرور قوية
  - ❖ يجب أن يغير المستخدم كلمة المرور في أول دخول له
- في حال معرفة أو اكتشاف كلمات المرور، يجب اتخاذ الإجراءات التالية:
  - ❖ التحكم في كلمات المرور وحمايتها
  - ❖ تغيير كلمة المرور فوراً إلى كلمة مرور قوية.

إرشادات كلمة المرور

- يجب تغيير كلمات المرور كل 90 يوم على الأقل.
- يجب أن تكون كلمات المرور ذات 8 رموز أبجدي على الأقل
- يجب أن تحوي كلمات المرور مزيج من الحروف الكبيرة والحروف الصغيرة ورقمين على الأقل. يجب ألا تكون الرموز الرقمية في بداية أو نهاية كلمة المرور. يجب تضمين الرموز الخاصة في كلمة المرور حيث يسمح نظام الحاسب. الحروف الخاصة هي:(! @# $٪ ^ & * _ + =؟/~ '::،<>| \).
- يجب ألا تكون كلمات المرور سهلة التخمين وألا تكون:
  - اسم المستخدم الخاص بك.
  - رقم التوظيف لديك.
  - ألا تكون اسمك.
  - ألا يكون اسم من أفراد العائلة.
  - ألا تكون اسمك المستعار.
  - ألا يكون رقمك الشخصي.
  - ألا تكون تاريخ ميلادك.
  - ألا تكون رقم لوحة سيارتك.
  - ألا تكون عنوانك.
  - ألا تكون رقم هاتفك.
  - ألا تكون اسم مدينتك.
  - ألا تكون اسم القسم أو الإدارة لديك.
  - ألا تكون اسم شارع
  - ألا تكون اسم أو موديل سيارة.
  - ألا تكون كلمة عامية.
  - ألا تكون مصطلح فني.
  - ألا يكون اسم مدرسة أو شعار مدرسة.
  - ألا تكون أي معلومات عنك يسهل معرفتها (اللون أو الطعام أو الرياضة المفضلة لديك إلخ) .
  - ألا تكون اختصارات شائعة.
  - ألا تكون كلمات في القاموس
  - ألا تكون عكس لأي كلمة سبق وصفها أعلاه
- يجب عدم إعادة استخدام كلمات المرور لمدة عام واحد.
- يجب عدم مشاركة كلمات المرور مع أي شخص.
- يجب معاملة كلمات المرور كمعلومات سرية.

إنشاء كلمة مرور قوية

- دمج كلمات قصيرة وغير متصلة مع أرقام أو رموز خاصة. على سبيل المثال:eAt42peN
- لتكن كلمة المرور صعبة التخمين ولكن يسهل تذكرها.
- قم باستبدال الأرقام أو الرموز الخاصة للحروف. (ولكن ليس مجرد بديل) على سبيل المثال:
  - livefish- هي كلم مرور فاشلة.
  - L1veF1sh- هي كلمة أفضل وتناسب القواعد ولكنها تضع نمط الحرف الأول الاستهلالي ويمكن تخمين استبدالها بالرقم 1
  - v3f1Sh !l-أفضل بكثير ولا يمكن توقع كتابة الحروف بطريقة استهلالية واستبدال الرموز.

الإجراءات التأديبية:	قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع الموظف.
معلومات مساعدة	يتم تدعيم السياسة الأمنية هذه بواسطة معايير السياسة الأمنية الآتية

رقم المرجع	تفاصيل معايير السياسة
1	عدم تجاوز أو تعطيل ضوابط أمن موارد المعلومات
2	يجب تأكيد وتعزيز وتحديث والمصادقة باستمرار على الوعي الأمني للعاملين.
3	يتحمل جميع العاملين مسؤولية إدارة استخدام موارد المعلومات ويخضعوا للمسائلة عن أفعالهم المتعلقة بأمن موارد المعلومات كما يتحمل العاملون أيضا على حد سواء مسؤولية الإبلاغ عن أي انتهاكات مشتبه فيها أو مؤكدة لهذه السياسة إلى الإدارة المختصة.
4	يتحمل جميع العاملين مسؤولية حماية كلمات المرور وأرقام الهوية الشخصية ويخضعوا للمسائلة عن أفعالهم المتعلقة بإفشاء كلمات المرور الخاصة بهم أو الخاصة بالغير داخل مؤسسة عيد الخيرية، يجب الإبلاغ عن جميع المخالفات الأمنية إلى المسؤول أو الإدارة المختصة.
5	تأمين الوصول إلى والتغيير إلى واستخدام موارد المعلومات على نحو صارم. يجب فحص سلطة الوصول إلى المعلومات لجميع المستخدمين على نحو منتظم، بالإضافة إلى تغيير الحالة الوظيفية على سبيل المثال: التنقل أو الترقية أو خفض المنصب أو الدرجة أو إنهاء الخدمة.
9	عند إنهاء العلاقة مع مؤسسة عيد الخيرية، على المستخدمين تسليم جميع العهد ومصادر المعلومات التي تديرها المؤسسة. تنطبق جميع السياسات الأمنية لمصادر المعلومات التابعة لمؤسسة عيد الخيرية وتظل سارية في حالة إنهاء العلاقة حتى يتم إجراء مثل هذا التسليم. علاوة على ذلك، تظل هذه السياسة سارية بعد إنهاء العلاقة.
16	رئيس قسم البنية التحتية والشبكات مسؤول عن تحديد صلاحيات الوصول إلى البرمجيات وأماكن تخزين البيانات المختلفة طبقاً لاحتياجات كل إدارة

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية
		2017/01/01	- منقحة
سياسة البريد الإلكتروني		خدمات المعلومات	-المحرر

مقدمة

مصادر المعلومات هي الأصول الاستراتيجية لمؤسسة عيد الخيرية والتي يجب أن تدار كمصادر ذات القيمة. وبالتالي تم تطوير هذه السياسة لتحقيق ما يلي:

- إرساء الممارسات الحكيمة والمقبولة فيما يتعلق باستخدام البريد الإلكتروني.
- توعية الأفراد باستخدام البريد الإلكتروني فيما يتعلق بمسؤولياتهم المرتبطة بهذا الاستخدام.

الغرض

الغرض من سياسة البريد الإلكتروني بمؤسسة عيد الخيرية هو إرساء القواعد لاستخدام البريد الإلكتروني بمؤسسة عيد الخيرية لإرسال واستقبال أو تخزين البريد الإلكتروني.

الجمهور

تنطبق سياسة البريد الإلكتروني بمؤسسة عيد الخيرية بالتساوي على جميع الأفراد الذين منحوا امتيازات الوصول إلى أي من موارد المعلومات بمؤسسة عيد الخيرية مع القدرة على إرسال أو استلام أو تخزين البريد الإلكتروني.

تعاريف

مصادر المعلومات (IR): أي من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

نظام البريد الإلكتروني: أي تطبيق لبرمجيات الحاسوب التي تسمح بتواصل البريد الإلكتروني من نظام حوسبة إلى آخر.

البريد الإلكتروني: أي رسالة أو صورة أو نموذج أو مرفق أو البيانات أو أي مراسلات أخرى يتم إرسالها أو استلامها أو تخزينها داخل نظام البريد الإلكتروني.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية
		2017/01/01	- منقحة
سياسة البريد الإلكتروني		خدمات المعلومات	-المحرر

سياسة البريد الإلكتروني

- تحظر هذه السياسة الأنشطة التالية:
  - ❖ إرسال رسالة باستخدام البريد الإلكتروني القصد منها التخويف أو المضايقة.
  - ❖ استخدام البريد الإلكتروني لإجراء الأعمال التجارية الشخصية.
  - ❖ استخدام البريد الإلكتروني لأغراض الضغط السياسي أو الحملات الانتخابية.
  - ❖ انتهاك قوانين حقوق التأليف والنشر عن طريق توزيع المصنفات المحمية بشكل غير لائق.
  - ❖ التظاهر بأنه شخص أخر عند إرسال البريد الإلكتروني، إلا عندما يصرح بإرسال رسائل أخرى عند القيام بدور دعم إداري.
  - ❖ استخدام برمجيات البريد الإلكتروني غير المصرح بها.

- تحظر الأنشطة التالية لأنها تعوق أداء شبكة الاتصالات وكفاءة عمليات نظم البريد الإلكتروني:
  - ❖ إرسال أو إعادة توجيه سلسلة خطابات.
  - ❖ إرسال الرسائل غير المرغوب فيها لمجموعات كبيرة باستثناء كما هو مطلوب للقيام بأعمال الوكالة.
  - ❖ إرسال رسائل كبيرة بشكل مفرط
  - ❖ إرسال أو إعادة توجيه رسالة البريد الإلكتروني التي من المحتمل أن تحتوي على فيروسات.

- تخضع جميع أنشطة المستخدم المتعلقة بأصول مصادر معلومات مؤسسة عيد الخيرية لإجراء تسجيل الدخول والاستعراض.

- لا يتصرف مستخدمي البريد الإلكتروني بشكل يعطي الانطباع بأنهم يمثلون أو يبدون الآراء أو خلاف ذلك يدلون ببيانات باسم مؤسسة عيد الخيرية أو أي من وحداتها إلا إذا صرح لهم القيام بذلك بشكل مناسب (صراحة أو ضمناً). حيثما كان ذلك مناسباً، يدرج تنازل صريح ما لم يكن واضحا من السياق أن المحرر لا يمثل مؤسسة عيد الخيرية. مثال على التنازل البسيط: "هذه الآراء المعرب عنها هي أرائي، وليست بالضرورة أراء صاحب العمل."

- لا يرسل الأفراد أو يعيدون توجيه أو يستلمون المعلومات الخاصة بمؤسسة عيد الخيرية من خلال حسابات بريد إلكتروني غير حسابات المؤسسة . تشمل أمثلة للأعمال حسابات البريد الإلكتروني لغير مؤسسة عيد الخيرية، ولكن لا تقتصر على: هوتميل أو بريد ياهو أو بريد جيميل أو أي بريد إلكتروني آخر غير بريد المؤسسة الرسمي(@eidcharity.net).

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية
		2017/01/01	- منقحة
سياسة البريد الإلكتروني		خدمات المعلومات	-المحرر

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع الموظف.

دعم المعلومات

تدعم سياسة الأمن معايير سياسة الأمن التالية.

مرجع #	تفاصيل معايير السياسة
3	يتحمل جميع العاملين مسؤولية إدارة استخدام مصادر المعلومات ويخضعوا للمساءلة عن أفعالهم المتعلقة بأمن مصادر المعلومات كما يتحمل العاملون أيضا على حد سواء مسؤولية الإبلاغ عن أي انتهاكات مشتبه فيها أو مؤكدة لهذه السياسة إلى الإدارة المختصة.
6	استخدام مصادر المعلومات لأغراض الأعمال المصرح بها رسميا فقط. لا يوجد ضمان للخصوصية الشخصية أو الوصول إلى أدوات والتي تتضمن على سبيل المثال لا الحصر، البريد الإلكتروني وتصفح الويب وأدوات المناقشة الإلكترونية الأخرى. قد يتم رصد استخدام أدوات التواصل الإلكتروني للوفاء بمتطلبات الشكوى أو التواصل مع المتبعرين والكفلاء .
7	إبقاء أي من البيانات المستخدمة في نظام مصادر المعلومات سرية وآمنة من قبل المستخدم ، وعلاوة على ذلك إذا تم تخزين هذه البيانات بشكل ورقي أو إلكتروني، أو إذا تم نسخ البيانات أو طباعتها أو نقلها إلكترونيا فينبغي حماية البيانات سرية وآمنة.
8	يجب حماية جميع برمجيات الحاسوب والتطبيقات والتعليمات البرمجية المصدر والوثائق والبيانات وتكون من مسؤولية رئيس قسم البنية التحتية والشبكات.

إدارة نظم المعلومات	سياسات أمن خدمات المعلومات	2012/01/01	- سارية
		2017/01/01	- منقحة
سياسة **الإنترنت**		نظم المعلومات	-المحرر

مقدمة

مصادر المعلومات هي الأصول التي يجب أن تدار كمصادر ذات القيمة. وبالتالي تم تطوير هذه السياسة لتحقيق ما يلي:

- ضمان الامتثال للقوانين المعمول بها واللوائح والتفويضات فيما يتعلق بإدارة مصادر المعلومات.
- إرساء الممارسات الحكيمة والمقبولة فيما يتعلق باستخدام الإنترنت.
- توعية الأفراد الذين يستخدمون الإنترنت والشبكات الداخلية فيما يتعلق بمسؤولياتهم المرتبطة بهذا الاستخدام.

الجمهور

تنطبق سياسة الإنترنت بمؤسسة عيد الخيرية على جميع الأفراد الذين منحوا الوصول إلى أي من مصادر المعلومات بمؤسسة عيد الخيرية مع القدرة على الوصول إلى الإنترنت والشبكات الداخلية أو كليهما.

تعاريف

مصادر المعلومات (IR): أي من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

إدارة نظم المعلومات	سياسات أمن خدمات المعلومات	2012/01/01	- سارية
		2017/01/01	- منقحة
سياسة **الإنترنت**		نظم المعلومات	-المحرر

تعاريف، تابع

موظف أمن المعلومات : مسؤول عن إدارة مهام أمن المعلومات داخل المؤسسة. وهو نقطة الاتصال الداخلية والخارجية لجميع المسائل المتصلة بأمن معلومات المؤسسة.

الإنترنت: نظام عالمي للربط بين أجهزة وشبكات الحاسوب. تمتلك أجهزة وشبكات الحاسوب بشكل منفصل مجموعة كبيرة من المنظمات والوكالات الحكومية والشركات والكليات. وتعد شبكة الإنترنت هي طريق المعلومات الفائق السرعة الحالي

الشبكات الداخلية (إنترانت): ترتكز الشبكة الخاصة الاتصالات وتبادل المعلومات- مثل شبكة الإنترنت- على بروتوكول التحكم بالإرسال/ برتوكول الإنترنت (TCP/IP)، ولكن يمكن للمستخدمين داخل المنظمة فقط الوصول إليها. عادة ما تكون الشبكات الداخلية (الإنترانت) للمنظمة محمية من الوصول الخارجي بواسطة جدار حماية.

الشبكة العنكبوتية العالمية: نظام مستضيفات المواقع والتي تدعم المستندات المنسقة بصيغة HTML (لغة ترميز النصوص التشعبية) وتحتوي على روابط إلى مستندات أخرى (روابط كثيفة التشعب) وملفات الصوت والفيديوهات والصور المرسومة. يمكن للمستخدمين دخول شبكة الإنترنت من خلال استخدام التطبيقات الأخرى التي تسمى المتصفحات مثل جوجل كروم وسفاري وفاير فوكس ومايكروسوفت إنترنت إكسبلورر

البائع: هو الشخص الذي يتبادل البضائع أو الخدمات من أجل المال.

الملكية

تعتبر جميع الملفات الإلكترونية التي تم إنشاؤها أو تم إرسالها أو استلامها أو تخزينها على الحواسيب المملوكة أو المؤجرة أو المدارة أو خلاف ذلك بموجب حفظ ومراقبة مؤسسة عيد الخيرية، هي ملك للمؤسسة.

الخصوصية

تعتبر الملفات الإلكترونية التي تم إنشائها، أو تم إرسالها أو استلامها أو تخزينها على الحواسيب المملوكة أو المؤجرة إدارياً أو خلاف ذلك ، والتي تخضع لمراقبة مؤسسة عيد الخيرية، غير خصوصية ويمكن لموظفي سياسات الخصوصية لمؤسسة عيد الخيرية الدخول عليها في أي وقت دون معرفة مستخدم مصادر المعلومات أو المالك.

إدارة نظم المعلومات	سياسات أمن خدمات المعلومات	2012/01/01	- سارية
		2017/01/01	- منقحة
سياسة **الإنترنت**		نظم المعلومات	-المحرر

سياسة استخدام الإنترنت والإنترانت

- يقدم برنامج تصفح الإنترنت للمستخدمين المرخص لهم لاستخدامه في العمل والأبحاث.
- يجب أن تكون جميع البرامج المستخدمة للوصول إلى الإنترنت جزءا من مجموعة البرمجيات القياسية في مؤسسة عيد الخيرية أو التي وافق عليها موظف أمن المعلومات.
- يجب مسح جميع الملفات التي تم تحميلها من الإنترنت للبحث عن الفيروسات باستخدام برمجيات أمن المعلومات وبرمجيات الكشف عن الفيروسات الحالية.
- يجب أن تمتثل جميع المواقع التي يتم الوصول إليها مع سياسات الاستخدام المقبولة في مؤسسة عيد الخيرية.
- تخضع جميع أنشطة المستخدم المتعلقة بأصول مصادر معلومات مؤسسة عيد الخيرية لإجراء تسجيل الدخول والاستعراض.
- يجب أن يتماشى محتوى جميع المواقع التابعة لمؤسسة عيد الخيرية مع سياسات الاستخدام المقبولة في المؤسسة.
- لا يجوز إدخال أي مواد مسيئة أو مزعجة عبر مواقع مؤسسة عيد الخيرية.
- لا يجوز إدخال أي إعلانات تجارية شخصية عبر مواقع مؤسسة عيد الخيرية.
- لا يجوز استخدام الوصول إلى شبكة الإنترنت في مؤسسة عيد الخيرية للحصول على مكاسب شخصية أو استدراج العروض لغير مؤسسة عيد الخيرية.
- لا يجوز عرض أي بيانات عبر مواقع مؤسسة عيد الخيرية دون التأكد من أن هذه المواد متاحة للأفراد أو المجموعات المرخص لها فقط.
- تخضع الملفات الإلكترونية لنفس قواعد سجلات الحفظ التي تنطبق على الوثائق الأخرى ويجب الحفاظ عليها.

إدارة نظم المعلومات	سياسات أمن خدمات المعلومات	2012/01/01	- سارية
		2017/01/01	- منقحة
سياسة **الإنترنت**		نظم المعلومات	-المحرر

الاستخدام العرضي

- يقتصر الاستخدام العرضي الشخصي للوصول إلى شبكة الإنترنت على المستخدمين المرخص لهم في مؤسسة عيد الخيرية، ولا يمتد ليشمل أفراد الأسرة أو المعارف.
- يجب ألا يؤدي الاستخدام العرضي إلى تحمل مؤسسة عيد الخيرية لأي تكاليف مباشرة.
- يجب ألا يتداخل الاستخدام العرضي مع أداء الواجبات العادية لعمل الموظف.
- عدم إرسال أو استلام ملفات أو وثائق قد تسبب المسؤولية القانونية أو أحراج لمؤسسة عيد الخيرية.
- جميع الملفات والوثائق – بما في ذلك الوثائق والملفات الشخصية – مملوكة لمؤسسة عيد الخيرية ويمكن الوصول إليها وفقا لهذه السياسة.

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع الموظف.

إدارة نظم المعلومات	سياسات أمن خدمات المعلومات	2012/01/01	- سارية
		2017/01/01	- منقحة
سياسة **الإنترنت**		نظم المعلومات	-المحرر

دعم المعلومات **تدعم سياسة الأمن معايير سياسة الأمن التالية.**

مرجع #	تفاصيل معايير السياسة
3	يتحمل جميع العاملين مسؤولية إدارة استخدام مصادر المعلومات ويخضعوا للمساءلة عن أفعالهم المتعلقة بأمن مصادر المعلومات كما يتحمل العاملون أيضا على حد سواء مسؤولية الإبلاغ عن أي انتهاكات مشتبه فيها أو مؤكدة لهذه السياسة إلى الإدارة المختصة.
6	استخدام مصادر المعلومات لأغراض الأعمال المصرح بها رسميا فقط. لا يوجد ضمان للخصوصية الشخصية أو الوصول إلى أدوات والتي تتضمن على سبيل المثال لا الحصر، البريد الإلكتروني وتصفح الويب وأدوات المناقشة الإلكترونية الأخرى. قد يتم رصد استخدام أدوات التواصل الإلكتروني للوفاء بمتطلبات الشكوى أو التواصل مع المتبعرين والكفلاء .
7	إبقاء أي من البيانات المستخدمة في نظام مصادر المعلومات سرية وآمنة من قبل المستخدم ، وعلاوة على ذلك إذا تم تخزين هذه البيانات بشكل ورقي أو إلكتروني، أو إذا تم نسخ البيانات أو طباعتها أو نقلها إلكترونيا فينبغي حماية البيانات سرية وآمنة.
16	رئيس قسم البنية التحتية والشبكات مسؤول عن تحديد صلاحيات الوصول إلى البرمجيات وأماكن تخزين البيانات المختلفة طبقاً لاحتياجات كل إدارة.

إدارة	نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية	
			2017/01/01	-منقحة	
سياسة	أمن النسخ الاحتياطي		نظم المعلومات	-المحرر	

مقدمة

النسخ الاحتياطية الإلكترونية من اشتراطات العمل لتمكين استرداد البيانات والتطبيقات في حالة أي من الأحداث مثل الكوارث الطبيعية أو فشل محرك أقراص النظام أو التجسس أو أخطاء في إدخال البيانات أو أخطاء في عمليات النظام.

الغرض

الغرض من سياسة النسخ الاحتياطي/ خطة التعافي من الكوارث (DRP) في مؤسسة عيد الخيرية هو إرساء القواعد للنسخ الاحتياطي وتخزين المعلومات الإلكترونية.

الجمهور

تنطبق سياسة النسخ الاحتياطي/ خطة التعافي من الكوارث (DRP) في مؤسسة عيد الخيرية على جميع الأفراد المسؤولين عن تثبيت ودعم مصادر المعلومات، والأفراد المسؤولين عن أمن مصادر المعلومات والبيانات.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية
		2017/01/01	-منقحة
سياسة أمن النسخ الاحتياطي		نظم المعلومات	-المحرر

تعاريف

مصادر المعلومات (IR): أي من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

النسخ الاحتياطي: نسخ الملفات والطلبات لتجنب فقدان البيانات وتيسير الاسترداد في حالة تعطل النظام.

البائع: هو الشخص الذي يتبادل البضائع أو الخدمات من أجل المال.

الخدمات

قد تشتمل خدمات معلومات العقود القائمة على تخزين البيانات الاحتياطية خارج الموقع. ويمكن تمديد هذه الخدمات إلى جميع كيانات مؤسسة عيد الخيرية عند الطلب.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية
		2017/01/01	-منقحة
سياسة أمن النسخ الاحتياطي		نظم المعلومات	-المحرر

سياسة النسخ الاحتياطي

- يجب أن يكون تواتر ومدى النسخ الاحتياطي وفقا لأهمية المعلومات والمخاطر المقبولة التي يحددها صاحب البيانات.
- توثيق ومراجعة عملية النسخ الاحتياطي والاسترداد لمصادر معلومات مؤسسة عيد الخيرية لكل نظام بشكل دوري.
- يجب أن يكون المورد (الموردين) الذين يقومون بتخزين النسخ الاحتياطية خارج الموقع لمؤسسة عيد الخيرية موثوق بهم للتعامل مع أعلى مستوى من المعلومات المخزنة.
- تنفيذ عملية التحقق من نجاح النسخ الاحتياطي للمعلومات الإلكترونية لمؤسسة عيد الخيرية.
- اختبار النسخ الاحتياطية بشكل دوري للتأكد من أنها قابلة للاسترداد.
- مراجعة الإجراءات بين مؤسسة عيد الخيرية وموردي تخزين النسخ الاحتياطية خارج الموقع على الأقل مرة سنوياً في حالة التعامل مع مورد خارجي بهذا الخصوص.
- مراجعة دورية لسياسة النسخ الاحتياطية للخوادم الموجودة بمؤسسة عيد الخيرية طبقاً للأهمية والأولوية.
- يجب أن تشتمل أشرطة النسخ الاحتياطي على معايير التعريف التالية التي يمكن تحديدها بسهولة بالملصقات و/أو نظام الترميز:
  - اسم النظام
  - تاريخ الإنشاء

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع الموظف.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية
		2017/01/01	-منقحة
سياسة أمن النسخ الاحتياطي		نظم المعلومات	-المحرر

معلومات مساعدة تدعم سياسة الأمن معايير سياسة الأمن التالية.

مرجع #	تفاصيل معايير السياسة
7	إبقاء أي من البيانات المستخدمة في نظام مصادر المعلومات سرية وآمنة من قبل المستخدم ، وعلاوة على ذلك إذا تم تخزين هذه البيانات بشكل ورقي أو إلكتروني، أو إذا تم نسخ البيانات أو طباعتها أو نقلها إلكترونيا فينبغي حماية البيانات سرية وآمنة.
9	عند إنهاء العلاقة مع مؤسسة عيد الخيرية، على المستخدمين تسليم جميع العهد ومصادر المعلومات التي تديرها المؤسسة. تنطبق جميع السياسات الأمنية لمصادر المعلومات التابعة لمؤسسة عيد الخيرية وتظل سارية في حالة إنهاء العلاقة حتى يتم إجراء مثل هذا التسليم. علاوة على ذلك، تظل هذه السياسة سارية بعد إنهاء العلاقة.
11	يجب أن تتخذ الإدارة التي تطلب وتصرح بأحد تطبيقات الحاسوب الخطوات المناسبة لضمان سلامة وأمن جميع البرامج وملفات البيانات التي تم إنشاؤها.
14	سلامة استخدام البرمجيات والأجهزة، ونظم التشغيل والشبكات وملفات البيانات العامة هي مسؤولية رئيس قسم البنية التحتية والشبكات.
16	رئيس قسم البنية التحتية والشبكات مسؤول عن تحديد صلاحيات الوصول إلى البرمجيات وأماكن تخزين البيانات المختلفة طبقاً لاحتياجات كل إدارة.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية
		2017/01/01	-منقحة
سياسة أمن النسخ الاحتياطي		نظم المعلومات	-المحرر

دعم المعلومات، تابع تدعم سياسة الأمن معايير سياسة الأمن التالية.

مرجع #	تفاصيل معايير السياسة
17	تقييم جميع الإدارات بدقة لمخاطر التعديل غير المصرح به أو الإفشاء غير المصرح به أو فقدان البيانات التي تقع ضمن مسؤوليتهم وتضمن من خلال استخدام نظم الرصد حماية مؤسسة عيد الخيرية من الضرر أو المخاطر النقدية أو خلاف ذلك. تحتفظ إدارات المالك وأمين الحفظ بالنسخ الاحتياطية وخطط الطوارئ المناسبة للتعافي من الكوارث استناداً إلى متطلبات تقييم المخاطر والأعمال.
18	جميع عقود أنظمة الحاسوب والإيجارات والتراخيص والترتيبات الاستشارية أو غيرها من الاتفاقات يجب أن يصرح بها ويوقعها الموظف المفوض في مؤسسة عيد الخيرية ويجب أن تحتوي على الشروط التي أقرتها إدارة الشؤون القانونية، وتقديم المشورة إلى موردي مصادر معلومات مؤسسة عيد الخيرية المحتفظة بحقوق الملكية والحقوق المكتسبة فيما يتعلق بنظم المعلومات والبرامج ومتطلبات البيانات لأمن نظم الحاسوب، بما في ذلك حفظ واسترداد البيانات.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	-سارية
		2017/01/01	-تم مراجعتها
سياسة أمان الوصول إلى الشبكة		نظم المعلومات	-المحرر

مقدمة

يتم توفير البنية الأساسية لشبكة مؤسسة عيد الخيرية كأداة مركزية لكافة المستخدمين بإدارة مصادر المعلومات بالمؤسسة. وانه لمن الضروري أن تستمر البنية التحتية -التي تشمل على الكابلات والمعدات النشطة المرتبطة بها - في التطور بمرونة كافية حتى ترضي احتياجات مؤسسة عيد الخيرية، بينما في الوقت نفسه تبقى قادرة على استغلال التطورات المتوقعة في تكنولوجيا الشبكات عالية السرعة لتسمح بتوفير خدمات محسنة للمستخدم.

الغرض

الغرض من سياسة الوصول إلى شبكة مؤسسة عيد الخيرية هو إرساء قواعد للوصول إلى البنية التحتية للشبكة واستخدامها. وهذه القواعد ضرورية للحفاظ على سلامة وتوافر وسرية المعلومات الخاصة بالمؤسسة.

الجمهور

تُطبق سياسة الوصول لشبكة مؤسسة عيد الخيرية على جميع الأفراد الذين لديهم تصريح للوصول لمصادر معلومات المؤسسة.

تعاريف

مصادر المعلومات (IR): كل من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

تعاريف، تابع

موظف أمن المعلومات : مسؤول عن إدارة مهام أمن المعلومات داخل المؤسسة. وهو نقطة الاتصال الداخلية والخارجية لجميع المسائل المتصلة بأمن معلومات المؤسسة.

إدارة نظم المعلومات : اسم الإدارة المسؤولة عن الحواسيب وشبكة الإنترنت وإدارة البيانات.

سياسة الوصول إلي الشبكة

- لا يسمح للمستخدمين باستخدام أي عناوين إلا عناوين تلك الشبكات الصادرة لهم بواسطة إدارة نظم المعلومات بمؤسسة عيد الخيرية.
- تكون جميع خدمات الوصول عن بعد (خدمات الاتصال) بمؤسسة عيد الخيرية إما عن طريق مجمع مودم أو موفر خدمة إنترنت.
- لا يمكن اتصال المستخدمين عن بعد بمؤسسة عيد الخيرية إلا من خلال موفر خدمة إنترنت واستخدام بروتوكولات تم الموافقة عليها بواسطة إدارة نظم المعلومات بمؤسسة عيد الخيرية.
- لا يجوز للمستخدمين داخل جدار الحماية بمؤسسة عيد الخيرية بالاتصال بشبكة المؤسسة في نفس الوقت الذي يستخدم فيه مودم للاتصال بشبكة اتصال خارجية.
- لا يجب على المستخدمين تمديد أو إعادة نقل خدمات الشبكات بأي شكل من الأشكال. وهذا يعني أنه لا يجب تثبيت جهاز التوجيه أو التبديل أو محور الوصل أو نقطة الوصول اللاسلكية بالشبكة الخاصة بمؤسسة عيد الخيرية دون موافقة إدارة نظم المعلومات بالمؤسسة.
- لا يسمح للمستخدمين بتثبيت شبكة الأجهزة أو البرامج التي توفر خدمات الشبكة دون موافقة إدارة نظم المعلومات بمؤسسة عيد الخيرية.
- يجب أن تطابق الأنظمة الحاسوبية الغير تابعة إلى مؤسسة العيد الخيرية التي تتطلب الاتصال بالشبكة معايير إدارة نظم المعلومات بالمؤسسة.
- لا يسمح للمستخدمين بتحميل أو تثبيت أو تشغيل برامج أو خدمات حماية، التي تكشف نقاط الضعف في أمن نظام ما. فعلى سبيل المثال، لا يسمح لمستخدمين مؤسسة عيد الخيرية بتشغيل برامج فك كلمة المرور أو التلصص على كتل المعلومات أو استخدام أدوات تصميم الشبكات أو جهاز كشف المنافذ عند الاتصال بأي طريقة بالبنية الأساسية لشبكة مؤسسة عيد الخيرية.
- لا يسمح للمستخدمين تعديل أو تغيير أجهزة الشبكة بأي شكل من الأشكال.

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع المظف.

معلومات الدعم **يتم دعم السياسة الأمنية بواسطة معايير السياسة الأمنية التالية**

مرجع #	تفاصيل معايير السياسة
1	عدم تجاوز أو تعطيل ضوابط أمن موارد المعلومات
3	يتحمل جميع العاملين مسؤولية إدارة استخدام مصادر المعلومات ويخضعوا للمساءلة عن أفعالهم المتعلقة بأمن مصادر المعلومات كما يتحمل العاملون أيضا على حد سواء مسؤولية الإبلاغ عن أي انتهاكات مشتبه فيها أو مؤكدة لهذه السياسة إلى الإدارة المختصة.
5	يجب مراجعة صلاحيات وصول المستخدمين بصفة دورية إلى مصادر المعلومات بما في ذلك التغييرات التي قد تحدث على الموظفين مثل التنقل أو الترقية أو خفض المنصب أو الدرجة أو إنهاء الخدمة.
6	استخدام مصادر المعلومات لأغراض الأعمال المصرح بها رسميا فقط. لا يوجد ضمان للخصوصية الشخصية أو الوصول إلى أدوات والتي تتضمن على سبيل المثال لا الحصر، البريد الإلكتروني وتصفح الويب وأدوات المناقشة الإلكترونية الأخرى. قد يتم رصد استخدام أدوات التواصل الإلكتروني للوفاء بمتطلبات الشكوى أو التواصل مع المتبعرين والكفلاء .
20	يجب أن يتوافق الوصول الخارجي من وإلى موارد المعلومات مع التوجهات الأمنية المناسبة المنشورة من قبل المؤسسة.

المراجع

قانون حقوق الطبع والنشر لعام 1976
قانون ممارسات الفساد الأجنبية لعام 1977
قانون الاحتيال وإساءة استعمال الكمبيوتر لعام 1986
قانون أمن الكمبيوتر لعام 1987
قانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة لعام 1996 (HIPAA)
قانون المعلومات في ولاية تكساس
قانون حكومة تكساس، القسم 441
القانون الإداري في تكساس، الفصل 202
قانون إدارة مصادر المعلومات، 2054.075(b)
قانون العقوبات في ولاية تكساس، الفصلين 33 و33أ
ممارسات إدارة مصادر المعلومات لحماية أصول مصادر المعلومات
استعراض معايير إدارة مصادر المعلومات ونشر التوصيات

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية
		2017/01/01	-تم مراجعتها
سياسة **إعداد الشبكة**		نظم المعلومات	-المحرر

مقدمة

يتم توفير البنية الأساسية لشبكة مؤسسة عيد الخيرية كأداة مركزية لكافة المستخدمين بإدارة مصادر المعلومات بمؤسسة عيد الخيرية. انه لمن الضروري أن تستمر البنية التحتية - التي تشمل على الكابلات والمعدات النشطة المرتبطة بها مثل أجهزة التوجيه والتحويل- في التطور بمرونة كافية حتى ترضي احتياجات المستخدمين، بينما في الوقت نفسه تبقى قادرة على استغلال التطورات المتوقعة في تكنولوجيا الشبكات عالية السرعة لتسمح بتوفير نظم محسنة للمستخدم.

الغرض

إن الغرض من سياسة أمن إعداد شبكة مؤسسة عيد الخيرية هو تحديد قواعد لصيانة وتمديد واستخدام البنية الأساسية للشبكة. وتعد هذه القواعد ضرورية للحفاظ على سلامة وتوافر وسرية المعلومات الخاصة بمؤسسة عيد الخيرية.

الجمهور

تطبق سياسة إعداد شبكة مؤسسة عيد الخيرية على جميع الأفراد الذين لديهم تصريح للوصول لمصادر معلومات مؤسسة عيد الخيرية.

تعاريف

مصادر المعلومات (IR): كل من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب النظم. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات

تعاريف، تابع

موظف أمن المعلومات: مسؤول عن إدارة مهام أمن المعلومات داخل المؤسسة. وهو نقطة الاتصال الداخلية والخارجية لجميع المسائل المتصلة بأمن معلومات المؤسسة.

إدارة نظم المعلومات : اسم الإدارة المسؤولة عن الحواسيب وشبكة الإنترنت وإدارة البيانات.

معايير ممارسة أمن إعداد الشبكة.

- تعد إدارة نظم المعومات هي المسؤولة عن البنية التحتية لشبكة عيد الخيرية، وعليها الإستمرار في إدارة المزيد من التطورات والتحسينات لهذه البنية التحتية.
- لتوفير بنية تحتية لشبكة مؤسسة عيد الخيرية تتميز بالاتساق وبإمكانها استغلال تطورات الشبكة الجديدة، يجب تثبيت جميع موصلات الكابل بواسطة نظم المعلومات لدى المؤسسة أو مقاول معتمد لديها.
- يجب إعداد جميع الأجهزة المتصلة بالشبكة بمواصفات معتمدة بواسطة نظم المعلومات لمؤسسة عيد الخيرية.
- تخضع جميع الأجهزة المتصلة بشبكة عيد الخيرية إلى إدارة نظم المعلومات للمؤسسة ومعايير مراقبتها.
- يجب عدم إجراء تغييرات على إعدادات أجهزة إدارة الشبكة النشطة دون موافقة نظم المعلومات لمؤسسة عيد الخيرية.
- تدعم البنية التحتية لشبكة عيد الخيرية مجموعة تم تعريفها لبروتوكولات الشبكة المعتمدة. يجب موافقة نظم المعلومات لمؤسسة عيد الخيرية بأي استخدام لبروتوكولات غير معرّفة.
- تُخصص عناوين الشبكة للبروتوكولات المدعومة وتُسجل ويتم إدارتها بواسطة نظم المعلومات لمؤسسة عيد الخيرية.
- تعد جميع التوصيلات بالبنية التحتية للشبكة إلى شبكة الغير الخارجية مسؤولية نظم المعلومات لمؤسسة عيد الخيرية. ويتضمن هذا التوصيلات بشبكات الهاتف الخارجية.
- يجب تثبيت وإعداد جدران حماية مصادر المعلومات لدى مؤسسة عيد الخيرية باتباع مستندات معايير تنفيذ جدران الحماية الخاصة بمؤسسة عيد الخيرية.
- لا يجب على المستخدمين تمديد أو إعادة نقل نظم الشبكات بأي شكل من الأشكال. وهذا يعني أنه لا يجب تثبيت جهاز التوجيه أوالتبديل أو محور الوصل أو نقطة الوصول اللاسلكية بالشبكة الخاصة بمؤسسة عيد الخيرية

دون موافقة إدارة نظم المعلومات بالمؤسسة.

- لا يسمح للمستخدمين بتثبيت شبكة الأجهزة أو البرامج التي توفر نظم الشبكة دون موافقة إدارة نظم المعلومات بمؤسسة عيد الخيرية.
- لا يسمح للمستخدمين تعديل أو تغيير أجهزة الشبكة بأي شكل من الأشكال.

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع المظف.

معلومات الدعم	يتم دعم السياسة الأمنية بواسطة معايير السياسة الأمنية التالية

مرجع #	تفاصيل معايير السياسة
12	تملك إدارة نظم المعلومات شبكة مصادر المعلومات وتتحكم فيها. يجب الحصول على موافقة من إدارة نظم المعلومات قبل توصيل جهاز لا يتطابق مع المبادئ التوجيهية المنشورة على الشبكة. يحق لإدارة أمن المعلومات فصل أي جهاز شبكة اتصال لا يمتثل للمعايير أو لا يعتبر آمناً على النحو الكاف.
15	تعتمد جميع التغييرات أو التعديلات على نظم موارد المعلومات والشبكات والبرامج أو البيانات من إدارة نظم المعلومات.
19	يجب أن تفي أنظمة حاسوب مصادر المعلومات و/أو الأجهزة الملحقة المستخدمة لأعمال المؤسسة الجارية أو التي يتم إدارتها خارج نطاق تحكم المؤسسة بالمتطلبات التعاقدية وتخضع للمراقبة.
20	يجب أن يتوافق الوصول الخارجي من وإلى موارد المعلومات مع التوجيهات الأمنية المناسبة المنشورة من قبل المؤسسة.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	-سارية
		2017/01/01	-تم مراجعتها
سياسة إدراج خادم جديد للشبكة		نظم المعلومات	-المحرر

مقدمة

يُعتمد على برامج الخادم في تقديم البيانات بطريقة آمنة وموثوق بها. ويجب أن يكون هناك ضمان بأنه يتم الحفاظ على سلامة البيانات وسريتها وتوافرها. ويُعد ضمان أن برامج الخادم تم تثبيتها وحفظها بطريقة تمنع الوصول أو الاستخدام الغير مصرح به وعدم انقطاع الخدمة أحد الخطوات المطلوبة لتحقيق هذا الضمان.

الغرض

يتمثل غرض وثيقة "سياسة زيادة حماية الخادم بمؤسسة عيد الخيرية " في وصف المتطلبات لتثبيت خادم جديد بطريقة آمنة والحفاظ على سلامة أمن الخادم وبرامج التطبيق.

الجمهور

تنطبق سياسة زيادة حماية الخادم بمؤسسة عيد الخيرية على جميع الأفراد المسؤولين عن تثبيت مصادر المعلومات الجديدة وعمليات مصادر المعلومات الحالية والأفراد المسؤولين عن أمن مصادر المعلومات.

تعاريف

مصادر المعلومات (IR): أي من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

المورد: هو الشخص الذي يتبادل البضائع أو الخدمات من أجل المال.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	-سارية
		2017/01/01	-تم مراجعتها
سياسة إدراج خادم جديد للشبكة		نظم المعلومات	-المحرر

تعاريف، تابع

إدارة نظم المعلومات: اسم الإدارة المسؤولة عن الحواسيب والشبكة وإدارة البيانات.

الخادم: جهاز حاسوبي يوفر خدمات لبرامج حاسوبية أخرى لنفس جهاز الكمبيوتر أو لجهاز كمبيوتر أخر. ويشار إلى الحاسوب الذي يقوم بتشغيل برنامج خادم في كثير من الأحيان على انه خادم، على الرغم من أنه قد يقوم بتشغيل برامج حاسوب (خادم) أخر.

موظف أمن المعلومات : مسؤول عن إدارة مهام أمن المعلومات داخل المؤسسة. وهو نقطة الاتصال الداخلية والخارجية لجميع المسائل المتصلة بأمن معلومات المؤسسة.

سياسة إدراج خادم جديد للشبكة.

- يجب التأكد من وجود المصادر اللازمة لإنشاء خادم جديد سواء إفتراضي أو حقيقي.
- يجب معرفة السبب الرئيسي من إنشاء الخادم والصلاحيات التي ستعطى للمستخدمين من خلال هذا الخادم.
- يجب وضع جميع الإحتياطات الأمنية ضد اختراق الخادم قبل تفعيله على الشبكة.
- يجب مراجعة جميع البرامج التي سيتم تحميلها على الخادم الجديد من قبل رئيس قسم البنية التحتية والشبكات.
- يجب اختبار كفائة وفاعلية الخادم قبل تفعيله على الشبكة.
- يجب التأكد من وضع الإحتياطات لعدم انقطاع الخدمة عن البرامج المرتبطة بالخادم.
- يجب معرفة آلية النسخ الاحتياطية للبيانات والبرامج المرتبطة بالخادم.

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع المظف.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	-سارية
		2017/01/01	-تم مراجعتها
سياسة إدراج خادم جديد للشبكة		نظم المعلومات	-المحرر

دعم المعلومات **تُدعم سياسة الأمن هذه بواسطة معايير سياسة الأمن التالية.**

مرجع #	تفاصيل معايير السياسة
8	يجب حماية جميع برمجيات الحاسوب والتطبيقات والتعليمات البرمجية المصدر والوثائق والبيانات وتكون من مسؤولية رئيس قسم البنية التحتية والشبكات.
11	يجب أن تتخذ الإدارة التي تطلب وتصرح بأحد تطبيقات الحاسوب الخطوات المناسبة لضمان سلامة وأمن جميع البرامج وملفات البيانات التي تم إنشاؤها
12	تملك إدارة نظم المعلومات شبكة مصادر المعلومات وتتحكم فيها. يجب الحصول على موافقة من إدارة نظم المعلومات قبل توصيل جهاز لا يتطابق مع المبادئ التوجيهية المنشورة على الشبكة. يحق لإدارة أمن المعلومات فصل أي جهاز شبكة اتصال لا يمتثل للمعايير أو لا يعتبر آمناً على النحو الكاف.
16	رئيس قسم البنية التحتية والشبكات مسؤول عن تحديد صلاحيات الوصول إلى البرمجيات وأماكن تخزين البيانات المختلفة طبقاً لاحتياجات كل إدارة.
17	تقييم جميع الإدارات بدقة لمخاطر التعديل غير المصرح به أو الإفشاء غير المصرح به أو فقدان البيانات التي تقع ضمن مسؤوليتهم وتضمن من خلال استخدام نظم الرصد حماية مؤسسة عيد الخيرية من الضرر أو المخاطر النقدية أو خلاف ذلك. تحتفظ إدارات المالك وأمين الحفظ بالنسخ الاحتياطية وخطط الطوارئ المناسبة للتعافي من الكوارث استناداً إلى متطلبات تقييم المخاطر والأعمال.

إدارة :نظم المعلومات المعلومات سياسة : **وصول مزودي الخدمة**	2012/01/01 2017/01/01 نظم المعلومات

مقدمة

يؤدي مزودو الخدمات دورًا مهمًا في دعم المكونات المادية للحاسوب وإدارة المكونات غير المادية والعمليات للعملاء. يمكن لمزودي الخدمات استعراض ونسخ وتعديل البيانات عن بعد وفحص السجلات، فهم يقوموا بضبط برمجيات الحاسوب وتشغيل مشاكل الأنظمة، كما يمكنهم المراقبة والموالفة الدقيقة لأداء الأنظمة، وأيضا يمكنهم مراقبة أداء المكونات المادية للحاسوب والأخطاء وتعديل الأنظمة البيئية . وضع الحدود والضوابط على ما يمكن رؤيته ونسخه وتعديله ومراقبته من جانب مزودي الخدمات سيقلل بالطبع خطر فقدان البيانات.

الغرض

إن الغرض من هذه السياسة هو إرساء قواعد وصول مزودي الخدمات لمصادر معلومات مؤسسة عيد الخيرية ودعم الخدمات وحماية المعلومات.

الجمهور

تتطبق سياسة **تسهيل وصول مزودي الخدمات** على جميع الأفراد المسؤولين عن تثبيت أصول مصادر المعلومات الجديدة والعمليات والحفاظ على مصادر المعلومات الحالية والذين يفعلوا أو قد يسمحوا بالوصول إلى مزودي الخدمات لأغراض الصيانة والمراقبة وتحرى الخلل وإصلاحه.

تعاريف

مصادر المعلومات (IR): أي من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

مزود الخدمة: هو الشخص الذي يتبادل البضائع أو الخدمات من أجل المال.

إدارة :نظم المعلومات المعلومات سياسة : **وصول مزودي الخدمة**	2012/01/01 2017/01/01 نظم المعلومات

سياسة وصول مزودي الخدمات

- يجب أن يمتثل مزودي الخدمات مع جميع سياسات مؤسسة عيد الخيرية المعمول بها، ومعايير الممارسات والاتفاقيات، على سبيل المثال لا الحصر:
  - ❖ سياسات السلامة
  - ❖ سياسات الخصوصية
  - ❖ السياسات الأمنية
  - ❖ سياسات التدقيق
  - ❖ سياسات ترخيص البرمجيات
  - ❖ سياسات الاستخدام المقبول
- يجب أن تحدد اتفاقيات وعقود مزودي الخدمة الآتي:
  - ❖ أن يتمكن مزود الخدمة من الوصول إلى معلومات مؤسسة عيد الخيرية.
  - ❖ كيفية حماية معلومات مؤسسة عيد الخيرية من جانب مزود الخدمة.
  - ❖ الأساليب المقبولة لعودة أو إتلاف أو التخلص من معلومات مؤسسة عيد الخيرية التي تكون في حيازة مزود الخدمة في نهاية العقد.
  - ❖ يجب على مزود الخدمة استخدام فقط معلومات مؤسسة عيد الخيرية ومصادر المعلومات لغرض العمل المكلف به فقط.
  - ❖ لا يجوز استخدام أي معلومات يحصل عليها مزود الخدمة لمؤسسة عيد الخيرية في إطار العقد للأغراض االتجارية أو إفشائها للآخرين.
- ستوفر مؤسسة عيد الخيرية نقطة اتصال لخدمات المعلومات لمزود الخدمة. سوف تعمل نقطة الاتصال مع مزود الخدمة للتأكد من امتثاله مع هذه السياسات.
- يجب أن يقوم جميع مزودي الخدمة بتزويد مؤسسة عيد الخيرية بقائمة بجميع الموظفين العاملين بالعقد.
- يجب على جميع مزودي الخدمة إعطاء تقارير عن جميع الحوادث الأمنية مباشرة إلى موظفي مؤسسة عيد الخيرية المختصين.
- يجب أن يتبع مزود الخدمة جميع عمليات مراقبة التغيير والإجراءات الخاصة بعيد الخيرية المعمول بها.

مؤسسة الشيخ عيد الخيرية
SHEIKH EID BIN MOHAMMAD AL-THANI CHARITABLE ASSOCIATION

إدارة :نظم المعلومات المعلومات سياسة : **وصول مزودي الخدمة**	2012/01/01 2017/01/01 نظم المعلومات

سياسة الوصول إلى المورد، تابع

- جميع معدات الصيانة الخاصة بمزودي الخدمة على شبكة عيد الخيرية والتي تصل إلى العالم الخارجي من خلال شبكة الإنترنت، أو خط الهاتف أو خط مؤجر، ستظل معطلة إلا في حالة استخدمها للصيانة.
- عند انصراف الموظف طرف مزود الخدمة عن العقد لأي سبب، سيضمن مزود الخدمة أنه يتم جمع جميع المعلومات الدقيقة وإرجاعها إلى مؤسسة عيد الخيرية أو التخلص منها في غضون 24 ساعة.
- يقوم مزود الخدمة بإرجاع أو إتلاف جميع المعلومات الخاصة بمؤسسة عيد الخيرية وتقديم شهادة خطية عن هذا الإرجاع أو الإتلاف في غضون 24 ساعة. عند انتهاء العقد أو عند طلب مؤسسة عيد الخيرية.
- يجب أن يتم جرد وترخيص جميع البرمجيات المستخدمة من جانب مزود الخدمة

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع الموظف.

إدارة :نظم المعلومات المعلومات سياسة : **وصول مزودي الخدمة**	2012/01/01 2017/01/01 نظم المعلومات

دعم المعلومات	يتم دعم السياسة الأمنية من جانب معايير السياسة الأمنية لتالية
مرجع #	تفاصيل معايير السياسة
1	عدم تجاوز أو تعطيل ضوابط أمن موارد المعلومات
2	يجب تأكيد وتعزيز وتحديث والمصادقة باستمرار على الوعي الأمني
3	يتحمل جميع العاملين مسؤولية إدارة استخدام مصادر المعلومات ويخضعوا للمساءلة عن أفعالهم المتعلقة بأمن مصادر المعلومات كما يتحمل العاملون أيضا على حد سواء مسؤولية الإبلاغ عن أي انتهاكات مشتبه فيها أو مؤكدة لهذه السياسة إلى الإدارة المختصة.
4	يتحمل جميع العاملين مسؤولية حماية كلمات المرور وأرقام الهوية الشخصية ويخضعوا للمسائلة عن أفعالهم المتعلقة بإفشاء كلمات المرور الخاصة بهم أو الخاصة بالغير داخل مؤسسة عيد الخيرية، يجب الإبلاغ عن جميع المخالفات الأمنية إلى المسؤول أو الإدارة المختصة.
5	يجب مراجعة صلاحيات وصول المستخدمين بصفة دورية إلى مصادر المعلومات بما في ذلك التغييرات التي قد تحدث على الموظفين مثل التنقل أو الترقية أو خفض المنصب أو الدرجة أو إنهاء الخدمة.
6	استخدام مصادر المعلومات لأغراض الأعمال المصرح بها رسميا فقط. لا يوجد ضمان للخصوصية الشخصية أو الوصول إلى أدوات والتي تتضمن على سبيل المثال لا الحصر، البريد الإلكتروني وتصفح الويب وأدوات المناقشة الإلكترونية الأخرى. قد يتم رصد استخدام أدوات التواصل الإلكتروني للوفاء بمتطلبات الشكوى أو التواصل مع المتبعرين والكفلاء .
7	إبقاء أي من البيانات المستخدمة في نظام مصادر المعلومات سرية وآمنة من قبل المستخدم ، وعلاوة على ذلك إذا تم تخزين هذه البيانات بشكل ورقي أو إلكتروني، أو إذا تم نسخ البيانات أو طباعتها أو نقلها إلكترونيا فينبغي حماية البيانات سرية وآمنة.

دعم المعلومات، تابع **يتم دعم السياسة الأمنية من جانب معايير السياسة الأمنية التالية**

مرجع #	تفاصيل المعايير السياسة
9	عند إنهاء العلاقة مع مؤسسة عيد الخيرية، على المستخدمين تسليم جميع العهد ومصادر المعلومات التي تديرها المؤسسة. تنطبق جميع السياسات الأمنية لمصادر المعلومات التابعة لمؤسسة عيد الخيرية وتظل سارية في حالة إنهاء العلاقة حتى يتم إجراء مثل هذا التسليم. علاوة على ذلك، تظل هذه السياسة سارية بعد إنهاء العلاقة.
16	رئيس قسم البنية التحتية والشبكات مسؤول عن تحديد صلاحيات الوصول إلى البرمجيات وأماكن تخزين البيانات المختلفة طبقاً لاحتياجات كل إدارة.
17	تقييم جميع الإدارات بدقة لمخاطر التعديل غير المصرح به أو الإفشاء غير المصرح به أو فقدان البيانات التي تقع ضمن مسؤوليتهم وتضمن من خلال استخدام نظم الرصد حماية مؤسسة عيد الخيرية من الضرر أو المخاطر النقدية أو خلاف ذلك. تحتفظ إدارات المالك وأمين الحفظ بالنسخ الاحتياطية وخطط الطوارئ المناسبة للتعافي من الكوارث استناداً إلى متطلبات تقييم المخاطر والأعمال.

إدارة نظم المعلومات	سياسات أمن خدمات المعلومات	2012/01/01	- سارية
		2017/01/01	- منقحة
سياسة سياسة إدارة الحوادث		نظم المعلومات	-المحرر

مقدمة

يواصل عدد الحوادث الأمنية والتكلفة الناتجة عن توقف العمل وإعادة الخدمة في التصاعد. يعد تطبيق سياسات الأمن المشدد ومنع الوصول غير الضروري للشبكات والحواسيب وتحسين الوعي الأمني لدى المستخدم والكشف المبكر عن الحوادث الأمنية والتخفيف من آثارها كبعض الإجراءات التي يمكن اتخاذها للحد من المخاطر وخفض التكلفة الناجمة عن الحوادث الأمنية.

الغرض

وتصف هذه الوثيقة الاحتياجات اللازمة للتعامل مع الحوادث الأمنية للحواسيب. وتشمل الحوادث الأمنية ولكن لا تقتصر على: الكشف عن الفيروس والفيروس المتنقل وفيروس حصان طروادة والاستخدام غير المصرح به لحسابات الحاسوب ونظم الحاسوب، فضلا عن الشكاوى المتعلقة بالاستخدام غير السليم لمصادر المعلومات على النحو المبين في سياسة البريد الإلكتروني وسياسة الإنترنت وسياسة الاستخدام المقبول.

الجمهور

تطبق سياسة إدارة الحادث لمؤسسة عيد الخيرية على جميع الأفراد المستخدمين لمصادر معلومات عيد الخيرية.

تعاريف

مصادر المعلومات (IR): كل من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

تعاريف، تابع

موظف أمن المعلومات : مسؤول عن إدارة مهام أمن المعلومات داخل المؤسسة. وهو نقطة الاتصال الداخلية والخارجية لجميع المسائل المتصلة بأمن معلومات المؤسسة.

فريق الاستجابة لحوادث الحاسوب : الموظفون المسؤولون عن تنسيق الاستجابة لحوادث أمن الحاسوب في المؤسسة

الفيروس: أحد البرامج التي تعلق نفسها بالملف القابل للتنفيذ أو التطبيق الضعيف وتسبب خطورة تتراوح حجمها من المزعج إلى المدمر للغاية. ينتشر الفيروس في الحاسوب عند فتح ملف مصاب .

الفيروس المتنقل: برنامج ينسخ نفسه في أماكن أخرى في نظام الحوسبة. هذه النسخ قد يتم إنشاؤها على نفس الحاسوب أو يتم إرسالها عبر شبكات الاتصال إلى الحواسيب الأخرى. . بعض الفيروسات المتنقلة تمثل تهديدات أمنية باستخدام الشبكات لنشر نفسها وتعطيل الشبكات من خلال التحميل الزائد عليها. الفيروس المتنقل مماثل للفيروس في أنه ينسخ نفسه، ولكنه يختلف في كونه لا يحتاج أن يعلق نفسه على ملفات أو قطاعات معينة على الإطلاق.

فيروس حصان طروادة: من البرامج الهدامة – وعادة ما يكون فيروس أو فيروس متنقل– مخفي في برنامج جذاب أو برنامج يبدو سليم مثل الألعاب أو برامج الرسومات. قد يتلقى الضحايا برنامج حصان طروادة عن طريق البريد الإلكتروني أو من خلال قرص مرن أو عن طريق الفلاش ، وغالباً من شخص أخر لا يدرك الأمر، أو قد يحدث ذلك من خلال تحميل ملف من موقع إلكتروني أو نشرة.

الحادث الأمني: يعني في عمليات المعلومات، تقييم حدث لمحاولات الدخول أو الدخول غير المصرح به أو هجوم معلومات على نظام المعلومات المؤتمت. ويشمل التصفح غير المصرح به أو التعطل أو الحرمان من الخدمة أو إدخال تغيير أو تدمير أو معالجة أو تخزين أو إخراج المعلومات أو تغييرات في أجهزة نظم المعلومات أو البرامج الثابتة أو خصائص البرمجيات بمعرفة أو بدون معرفة المستخدمين أو تعليماتهم أو قصدهم.

المورد: هو الشخص الذي يتبادل البضائع أو الخدمات من أجل المال.

سياسة إدارة الحوادث

- يقوم قسم البنية التحتية والشبكات في مؤسسة عيد الخيرية بأدوار ومسؤوليات محددة مسبقا قد يكون لها الأولوية على الواجبات العادية.
- في حالة الشك في أو التأكد من وقوع حادث أمني، مثل فيروس أو فيروس متنقل أو بريد إلكتروني خادع، أو اكتشاف أدوات القرصنة أو تغيير البيانات، وغيرها، يجب أن تتبع إجراءات إدارة الحادث المناسبة.
- موظف أمن المعلومات هو المسؤول عن إخطار مدير نظم المعلومات وفريق البنية التحتية والشبكات لحوادث الحاسوب والبدء في اتخاذ إجراءات إدارة الحادث المناسبة بما في ذلك الاستعادة كما تم تحديدها في إجراءات إدارة الحادث.
- موظف أمن المعلومات هو المسؤول عن تحديد الدليل المادي والإلكتروني الذي يتم تجميعه كجزء من التحقيق في الحادث.
- المصادر الفنية المناسبة في فريق البنية التحتية والشبكات لحوادث الحاسوب هي المسؤولة عن مراقبة إصلاح أو التخفيف من أي ضرر ناتج عن وقوع حادث أمني والتخلص أو التقليل من هذا الخلل إذا كان ذلك ممكنا.
- يحدد موظف أمن المعلومات- الذي يعمل مع مدير نظم المعلومات- ما إذا كانت هناك حاجة إلى التواصل مع موظفي مؤسسة عيد الخيرية على نطاق واسع وما هو محتوى هذا التواصل وما هي أفضل السبل لتوزيع المراسلات.
- المصادر الفنية المناسبة في فريق البنية التحتية والشبكات لحوادث الحاسوب هي المسؤولة عن إزالة أو تخفيف هذا الخلل.
- موظف أمن المعلومات هو المسؤول عن البدء في واستكمال وتوثيق تحقيق الحادث بمساعدة فريق البنية التحتيه والشبكات لحوادث الحاسوب
- موظف أمن المعلومات في مؤسسة عيد الخيرية هو المسؤول عن الإبلاغ عن الحادث إلى **مدير نظم المعلومات**.

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع المظف.

إدارة نظم المعلومات	سياسات أمن خدمات المعلومات	2012/01/01	- سارية
		2017/01/01	- منقحة
سياسة سياسة إدارة الحوادث		نظم المعلومات	-المحرر

دعم المعلومات **تدعم سياسة الأمن معايير سياسة الأمن التالية.**

مرجع #	تفاصيل مبادئ السياسة
3	يتحمل جميع العاملين مسؤولية إدارة استخدام مصادر المعلومات ويخضعوا للمساءلة عن أفعالهم المتعلقة بأمن مصادر المعلومات كما يتحمل العاملون أيضا على حد سواء مسؤولية الإبلاغ عن أي انتهاكات مشتبه فيها أو مؤكدة لهذه السياسة إلى الإدارة المختصة.
6	استخدام مصادر المعلومات لأغراض الأعمال المصرح بها رسميا فقط. لا يوجد ضمان للخصوصية الشخصية أو الوصول إلى أدوات والتي تتضمن على سبيل المثال لا الحصر، البريد الإلكتروني وتصفح الويب وأدوات المناقشة الإلكترونية الأخرى. قد يتم رصد استخدام أدوات التواصل الإلكتروني للوفاء بمتطلبات الشكوى أو التواصل مع المتبعرين والكفلاء .
7	إبقاء أي من البيانات المستخدمة في نظام مصادر المعلومات سرية وآمنة من قبل المستخدم ، وعلاوة على ذلك إذا تم تخزين هذه البيانات بشكل ورقي أو إلكتروني، أو إذا تم نسخ البيانات أو طباعتها أو نقلها إلكترونيا فينبغي حماية البيانات سرية وآمنة.
16	رئيس قسم البنية التحتية والشبكات مسؤول عن تحديد صلاحيات الوصول إلى البرمجيات وأماكن تخزين البيانات المختلفة طبقاً لاحتياجات كل إدارة.

دعم المعلومات، تابع **تدعم سياسة الأمن معايير سياسة الأمن التالية.**

مرجع #	تفاصيل معايير السياسة
21	دعم جميع البرمجيات التجارية المستخدمة في أنظمة الحاسوب من خلال اتفاقية ترخيص البرمجيات التي تصف على وجه التحديد حقوق الاستخدام والقيود المفروضة على المنتج. يتقيد العاملين بجميع اتفاقيات الترخيص، ويجب ألا ينسخوا البرمجيات المرخصة بصورة غير قانونية. يحتفظ مدير مصادر المعلومات من خلال أمن المعلومات بالحق في إزالة أي برمجيات غير مرخصة من أي نظام حاسوبي.
22	يحتفظ مدير مصادر المعلومات من خلال أمن المعلومات بالحق في إزالة أي برمجيات أو ملفات لا تتعلق بالعمل من أي نظام حاسوبي. وتشمل أمثلة الملفات أو البرمجيات التي لا تتعلق بالعمل ولكن لا تقتصر على: الألعاب والرسائل الفورية والبريد الإلكتروني التابع لبروتوكول مكتب البريد (POP) والملفات الصوتية وملفات الصور والبرامج المجانية والبرامج المشتركة.

إدارة نظم المعلومات	سياسة أمن خدمات المعلومات	2012/01/01	- سارية
		2017/01/01	-منقحة
سياسة **إدارة الحساب**		خدمات المعلومات	-المحرر

مقدمة

حسابات المستخدمين هي الوسيلة المستخدمة لمنح حق الوصول إلى مصادر معلومات مؤسسة عيد الخيرية. هذه الحسابات توفر وسيلة للمساءلة، ومفتاحاً لاستخدام مصادر المعلومات. وهذا يعني أن إنشاء ومراقبة ورصد كافة حسابات المستخدمين أمر بالغ الأهمية لأمن المعلومات.

الغرض

الغرض من سياسة أمن إدارة حساب مؤسسة عيد الخيرية هو وضع القواعد لإنشاء ورصد ومراقبة وإزالة حسابات المستخدم

الجمهور

تنطبق سياسة أمن إدارة حساب مؤسسة عيد الخيرية على جميع الأفراد الذين لديهم إذن الوصول إلى أية مصادر لمعلومات مؤسسة عيد الخيرية.

إدارة نظم المعلومات	سياسة أمن خدمات المعلومات	2012/01/01	- سارية
		2017/01/01	-منقحة
سياسة **إدارة الحساب**		خدمات المعلومات	-المحرر

تعاريف

مصادر المعلومات (IR): كل من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

تعاريف، تابع

موظف أمن المعلومات : مسؤول عن إدارة مهام أمن المعلومات داخل المؤسسة. وهو نقطة الاتصال الداخلية والخارجية لجميع المسائل المتصلة بأمن معلومات المؤسسة.

مدير النظام: هو الشخص المسؤول عن التشغيل الفاعل وصيانة مصادر المعلومات، بما في ذلك تنفيذ الإجراءات والضوابط القياسية لفرض سياسة الأمن بالمؤسسة.

سياسة إدارة الحساب

- ترتبط بكافة الحسابات التي تم إنشاؤها بالطلب والموافقة المناسبة من نظام أو خدمة مؤسسة عيد الخيرية.
- توعية كافة المستخدمين بأمن مصادر المعلومات واتفاقية عدم الافصاح المعتمدين في مؤسسة عيد الخيرية قبل منح حق الوصول إلى الحساب.
- تحدد جميع الحسابات الشخصية باستخدام اسم المستخدم الذي تم تعيينه.
- تحدد جميع كلمات المرور الافتراضية للحسابات وفقا لسياسة كلمة المرور بمؤسسة عيد الخيرية.
- يكون لجميع الحسابات مدة انتهاء لكلمة المرور التي تتوافق مع سياسة كلمة المرور بمؤسسة عيد الخيرية.
- تعطيل حسابات الأفراد الذين في فترة إجازة ممتدة (أكثر من 30 يوما).
- مسؤولي النظام أو الموظفين المعينين الآخرين:
  - هم المسؤولون عن إزالة حسابات الأفراد الذين تغيرت أدوارهم داخل مؤسسة عيد الخيرية أو تم فصلهم من منصبهم في المؤسسة.
  - يقدمون قائمة بالحسابات للنظم التي يديرونها عند طلب إدارة مؤسسة عيد الخيرية
  - يتعاونون مع إدارة مؤسسة عيد الخيرية المصرح لها بالتحقيق في الحوادث الأمنية

إدارة نظم المعلومات	سياسة أمن خدمات المعلومات	2012/01/01	- سارية
		2017/01/01	-منقحة
سياسة **إدارة الحساب**		خدمات المعلومات	-المحرر

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع الموظف.

إدارة نظم المعلومات	سياسة أمن خدمات المعلومات	2012/01/01	- سارية
		2017/01/01	-منقحة
سياسة **إدارة الحساب**		خدمات المعلومات	-المحرر

دعم المعلومات	تدعم سياسة الأمن معايير سياسة الأمن التالية.

مرجع #	تفاصيل معايير السياسة
1	عدم تجاوز أو تعطيل ضوابط أمن موارد المعلومات
2	يجب تأكيد وتعزيز وتحديث والمصادقة باستمرار على الوعي الأمني للعاملين.
3	يتحمل جميع العاملين مسؤولية إدارة استخدام مصادر المعلومات ويخضعوا للمساءلة عن أفعالهم المتعلقة بأمن مصادر المعلومات كما يتحمل العاملون أيضا على حد سواء مسؤولية الإبلاغ عن أي انتهاكات مشتبه فيها أو مؤكدة لهذه السياسة إلى الإدارة المختصة.
4	يتحمل جميع العاملين مسؤولية حماية كلمات المرور وأرقام الهوية الشخصية ويخضعوا للمسائلة عن أفعالهم المتعلقة بإفشاء كلمات المرور الخاصة بهم أو الخاصة بالغير داخل مؤسسة عيد الخيرية، يجب الإبلاغ عن جميع المخالفات الأمنية إلى المسؤول أو الإدارة المختصة.
5	يجب مراجعة صلاحيات وصول المستخدمين بصفة دورية إلى مصادر المعلومات بما في ذلك التغييرات التي قد تحدث على الموظفين مثل التنقل أو الترقية أو خفض المنصب أو الدرجة أو إنهاء الخدمة.
6	استخدام مصادر المعلومات لأغراض الأعمال المصرح بها رسميا فقط. لا يوجد ضمان للخصوصية الشخصية أو الوصول إلى أدوات والتي تتضمن على سبيل المثال لا الحصر، البريد الإلكتروني وتصفح الويب وأدوات المناقشة الإلكترونية الأخرى. قد يتم رصد استخدام أدوات التواصل الإلكتروني للوفاء بمتطلبات الشكوى أو التواصل مع المتبعرين والكفلاء .
7	إبقاء أي من البيانات المستخدمة في نظام مصادر المعلومات سرية وآمنة من قبل المستخدم ، وعلاوة على ذلك إذا تم تخزين هذه البيانات بشكل ورقي أو إلكتروني، أو إذا تم نسخ البيانات أو طباعتها أو نقلها إلكترونيا فينبغي حماية البيانات سرية وآمنة.

إدارة نظم المعلومات	سياسة أمن خدمات المعلومات	2012/01/01	- سارية
		2017/01/01	-منقحة
سياسة **إدارة الحساب**		خدمات المعلومات	-المحرر

دعم المعلومات، تابع

تدعم سياسة الأمن معايير سياسة الأمن التالية.

مرجع #	تفاصيل معايير السياسة
9	عند إنهاء العلاقة مع مؤسسة عيد الخيرية، على المستخدمين تسليم جميع العهد ومصادر المعلومات التي تديرها المؤسسة. تنطبق جميع السياسات الأمنية لمصادر المعلومات التابعة لمؤسسة عيد الخيرية وتظل سارية في حالة إنهاء العلاقة حتى يتم إجراء مثل هذا التسليم. علاوة على ذلك، تظل هذه السياسة سارية بعد إنهاء العلاقة.
16	رئيس قسم البنية التحتية والشبكات مسؤول عن تحديد صلاحيات الوصول إلى البرمجيات وأماكن تخزين البيانات المختلفة طبقاً لاحتياجات كل إدارة.
17	تقييم جميع الإدارات بدقة لمخاطر التعديل غير المصرح به أو الإفشاء غير المصرح به أو فقدان البيانات التي تقع ضمن مسؤوليتهم وتضمن من خلال استخدام نظم الرصد حماية مؤسسة عيد الخيرية من الضرر أو المخاطر النقدية أو خلاف ذلك. تحتفظ إدارات المالك وأمين الحفظ بالنسخ الاحتياطية وخطط الطوارئ المناسبة للتعافي من الكوارث استناداً إلى متطلبات تقييم المخاطر والأعمال.

إدارة	نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01 - سارية
سياسة	**الوصول المادي**		2017/01/01 -تم مراجعتها
		نظم المعلومات	-المحرر

مقدمة

قد يكون لفريق عمل الدعم الفني والقائمين بإدارة الأمن وإدارة النظام والأخرين متطلبات للدخول الفعلي المادي لمصادر المعلومات كجزء من عملهم. يعد منح والتحكم في ومراقبة الدخول المادي إلى خدمات مصادر المعلومات أمرًا في غاية الأهمية لبرنامج الأمن بشكل عام.

الغرض

إن غرض سياسة الدخول المادي الخاصة بمؤسسة عيد الخيرية هي تحديد قوانين المنح والتحكم في ومراقبة وإلغاء الدخول المادي إلى خدمات مصادر المعلومات.

الجمهور

تنطبق سياسة الدخول المادي في مؤسسة عيد الخيرية على جميع الأفراد المسؤولين عن تثبيت ودعم موارد المعلومات، والأفراد المسؤولين عن أمن موارد المعلومات وأصحاب البيانات.

تعاريف

مصادر المعلومات (IR): كل من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

إدارة نظم المعلومات: اسم الإدارة المسؤولة عن الحواسيب والشبكة وإدارة البيانات.

سياسة الوصول المادي

- يجب أن تمتثل جميع أنظمة الأمن المادي لجميع اللوائح المعمول بها .
- يجب توثيق وإدارة الدخول المادي إلى غرف مركز البيانات الخاص بالمؤسسة.
- يجب حماية جميع خدمات مصادر المعلومات بشكل مادي مقارنة بدرجة حساسية أو أهمية وظيفتها لدى مؤسسة عيد الخيرية.
- يجب منح الدخول إلى خدمات مصادر المعلومات عن طريق موظفي ومقاولي عيد الخيرية فقط والذين تتطلب مسؤوليات عملهم الدخول إلى هذه الأماكن.
- يجب أن تتضمن عملية الدخول الرئيسي إلى خدمات مصادر المعلومات موافقة الشخص المسؤول للخدمة.
- يجب أن يتلقى كل فرد تم منحه حق الدخول إلى خدمة مصادر المعلومات تدريبات إجراءات الطوارئ للخدمة، ويجب أن يتبع سياسات الدخول المتبعه.
- يجب عدم مشاركة أكواد الدخول أو منحها لأخرين على سبيل الاستعارة.
- يجب حذف الكود أو البصمه الخاصه بالشخص الذي انتهت صلاحية دخوله ألى مركز البيانات.
- ستتعقب جميع خدمات مصادر المعلومات التي تسمح للزائرين بالدخول عملية دخول الزائر في سجل الدخول/ الخروج.
- يجب حفظ سجلات الدخول لغرفة مصادر المعلومات للمراجعة الدورية بناء على مدى حساسية مصادر المعلومات الخاضعة للحماية.
- يجب أن يلغي الشخص المسؤول عن خدمة مصادر المعلومات حقوق دخول الأفراد الذين تغيرت أدوراهم في مؤسسة عيد الخيرية أو الذين انقضت علاقتهم بالمؤسسة.
- يجب أن يدخل مزودي خدمات نظم المعلومات إلى غرفة البيانات الرئيسية بصحبة موظف من إدارة نظم المعلومات بمؤسسة عيد الخيرية مخول له الدخول إلى تلك الغرفه.

تابع سياسة الدخول المادي

- يجب أن يراجع الشخص المسؤول عن خدمة مصادر المعلومات سجلات الدخول وسجلات الزائر للخدمة دوريًا وعليه التحقق في الدخول غير العادي.
- يجب أن يراجع الشخص المسؤول عن خدمة مصادر المعلومات حقوق الدخول للخدمة دوريًا ويلغي دخول الأفراد الذين لم يعد دخولهم مطلوبًا.

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع المظف.

معلومات الدعم

يتم دعم السياسة الأمنية بواسطة معايير السياسة الأمنية التالية

مرجع #	تفاصيل معايير السياسة
1	عدم تجاوز أو تعطيل ضوابط أمن موارد المعلومات
2	يجب تأكيد وتعزيز وتحديث والمصادقة باستمرار على الوعي الأمني للعاملين.
3	يتحمل جميع العاملين مسؤولية إدارة استخدام موارد المعلومات ويخضعوا للمسائلة عن أفعالهم المتعلقة بأمن موارد المعلومات كما يتحمل العاملون أيضا على حد سواء مسؤولية الإبلاغ عن أي انتهاكات مشتبه فيها أو مؤكدة لهذه السياسة إلى الإدارة المختصة.
4	يلزم حماية كلمات المرور وأرقام الهوية الشخصية (رقم التعريف الشخصي) والإجراءات الأمنية الأخرى لأنظمة الحاسوب والأجهزة، من جانب المستخدم الفردي من الاستخدام الناجم عن أو الإفشاء إلى أي فرد أخر أو منظمة. الإبلاغ عن جميع الانتهاكات الأمنية لإدارة أمين الحفظ أو مالك إدارة القسم.

دعم المعلومات، تابع

يتم دعم السياسة الأمنية بواسطة معايير السياسة الأمنية التالية

مرجع #	تفاصيل معايير السياسة
5	تأمين الوصول إلى والتغيير إلى واستخدام موارد المعلومات على نحو صارم. يجب فحص سلطة الوصول إلى المعلومات لجميع المستخدمين على نحو منتظم، بالإضافة إلى تغيير الحالة الوظيفية على سبيل المثال: التنقل أو الترقية أو خفض المنصب أو الدرجة أو إنهاء الخدمة.
8	يجب حماية جميع برامج الكمبيوتر والتطبيقات والتعليمات البرمجية المصدر ورمز الكائن والوثائق والبيانات وتكون تحت حراسة ومحمية كما لو كانت ملكا للدولة.
9	يجب على المستخدمين تسليم جميع العهد وموارد المعلومات التي تديرها المؤسسة. عند إنهاء العلاقة مع المؤسسة. تطبق جميع السياسات الأمنية لموارد المعلومات وتظل نافذة المفعول في حالة إنهاء العلاقة حتى يتم إجراء مثل هذا التسليم. بالإضافة إلى ذلك، تظل هذه السياسة سارية بعد إنهاء العلاقة.
16	يجب أن توفر إدارات أمين الحفظ ضوابط الوصول الكافية من أجل مراقبة الأنظمة لحماية البيانات والبرامج من إساءة استخدامها وفقا للاحتياجات التي تحددها إدارات المالك. يجب أن يتم توثيق الوصول وتصريحه وضبطه كما ينبغي
19	يجب أن تفي أنظمة حاسوب مصادر المعلومات و/أو الأجهزة الملحقة المستخدمة لأعمال المؤسسة الجارية أو التي يتم إدارتها خارج نطاق تحكم المؤسسة بالمتطلبات التعاقدية وتخضع للمراقبة.

المراجع

قانون حقوق الطبع والنشر لعام 1976
قانون ممارسات الفساد الأجنبية لعام 1977
قانون الاحتيال وإساءة استعمال الكمبيوتر لعام 1986
قانون أمن الكمبيوتر لعام 1987
قانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة لعام 1996 (HIPAA)
قانون المعلومات في ولاية تكساس
قانون حكومة تكساس، القسم 441
القانون الإداري لتكساس، الفصل 202
قانون إدارة مصادر المعلومات، 2054.075(b)
قانون العقوبات في ولاية تكساس، الفصلين 33 و 33أ
ممارسات إدارة مصادر المعلومات لحماية أصول مصادر المعلومات
استعراض معايير إدارة مصادر المعلومات ونشر التوصيات

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية
		2017/01/01	-تم مراجعتها
سياسة **أمن الحوسبة المحمولة**		نظم المعلومات	-المحرر

مقدمة

تتزايد أهمية وتوافر أجهزة الحاسوب المحمولة حيث يجعل الحجم الصغير وإمكانية تشغيل هذه الأجهزة الأكثر استحسانًا للاستبدال بأجهزة سطح المكتب التقليدية في عدد كبير من التطبيقات. على الرغم من هذا، قد تزيد إمكانية حمل هذه الأجهزة من المخاطر الأمنية على المجموعات التي تستخدم الأجهزة.

الغرض

إن غرض السياسة الأمنية للحوسبة المحمولة الخاصة بعيد الخيرية هي تحديد قواعد استخدام أجهزة الحوسبة المحمولة واتصالها بالشبكة. وتعد هذه القواعد ضرورية للحفاظ على سلامة وتوافر وسرية المعلومات الخاصة بمؤسسة عيد الخيرية.

الجمهور

تُطبق السياسة الأمنية للحوسبة المحمولة لمؤسسة عيد الخيرية بالتساوي على جميع الأفراد الذين يستخدمون أجهزة الحوسبة المحمولة ويدخلون على مصادر المعلومات الخاصة بالمؤسسة.

تعاريف

مصادر المعلومات (IR): كل من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية
		2017/01/01	-تم مراجعتها
سياسة **أمن الحوسبة المحمولة**		نظم المعلومات	-المحرر

تعاريف، تابع

موظف أمن المعلومات : مسؤول عن إدارة مهام أمن المعلومات داخل المؤسسة. وهو نقطة الاتصال الداخلية والخارجية لجميع المسائل المتصلة بأمن معلومات المؤسسة.

إدارة نظم المعلومات : اسم الإدارة المسؤولة عن الحواسيب والشبكة وإدارة البيانات.

أجهزة الحوسبة المحمولة: أي جهاز يسهل حمله ويمكن استلامه و/أو إرساله للبيانات من وإلى مصادر المعلومات. يتضمن هذا على سبيل المثال لا الحصر أجهزة الحاسوب المحمولة والجوالات.

سياسة الحوسبة المحمولة

- تُستخدم أجهزة الحوسبة المحمولة المعتمدة فقط لدى مؤسسة عيد الخيرية للدخول إلى مصادر معلومات المؤسسة.
- يجب حماية أجهزة الحوسبة المحمولة عن طريق كلمة مرور.
- لا يجب تخزين بيانات عيد الخيرية في أجهزة الكمبيوتر المحمولة.
- يجب عدم اتصال الأجهزة المحمولة الغير مرتبطة بالمؤسسة بالإنترنت إلا بإذن من مدير إدارة نظم المعلومات.
- يجب تشغيل برامج المؤسسة على الأجهزة المحمولة فقط أثناء تواجد الجهاز داخل المؤسسة ولا يمكن تشغيل تلك البرامج خارج المؤسسة.
- يجب أن تتبع جميع الأجهزة المحمولة سياسة الحماية من الفيروسات المتبعه داخل المؤسسة.

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع المظف.

معلومات الدعم **يتم دعم السياسة الأمنية بواسطة معايير السياسة الأمنية التالية**

مرجع #	تفاصيل معايير السياسة
1	عدم تجاوز أو تعطيل ضوابط أمن موارد المعلومات
3	يتحمل جميع العاملين مسؤولية إدارة استخدام مصادر المعلومات ويخضعوا للمساءلة عن أفعالهم المتعلقة بأمن مصادر المعلومات كما يتحمل العاملون أيضا على حد سواء مسؤولية الإبلاغ عن أي انتهاكات مشتبه فيها أو مؤكدة لهذه السياسة إلى الإدارة المختصة.
5	يجب مراجعة صلاحيات وصول المستخدمين بصفة دورية إلى مصادر المعلومات بما في ذلك التغييرات التي قد تحدث على الموظفين مثل التنقل أو الترقية أو خفض المنصب أو الدرجة أو إنهاء الخدمة.
7	إبقاء أي من البيانات المستخدمة في نظام مصادر المعلومات سرية وآمنة من قبل المستخدم ، وعلاوة على ذلك إذا تم تخزين هذه البيانات بشكل ورقي أو إلكتروني، أو إذا تم نسخ البيانات أو طباعتها أو نقلها إلكترونيا فينبغي حماية البيانات سرية وآمنة.
12	تملك إدارة نظم المعلومات شبكة مصادر المعلومات وتتحكم فيها. يجب الحصول على موافقة من إدارة نظم المعلومات قبل توصيل جهاز لا يتطابق مع المبادئ التوجيهية المنشورة على الشبكة. يحق لإدارة أمن المعلومات فصل أي جهاز شبكة اتصال لا يمتثل للمعايير أو لا يعتبر آمناً على النحو الكاف.
20	يجب أن يتوافق الوصول الخارجي من وإلى موارد المعلومات مع التوجيهات الأمنية المناسبة المنشورة من قبل المؤسسة.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية
		2017/01/01	- منقحة
سياسة **المراقبة الأمنية**		نظم المعلومات	-المحرر

مقدمة

إن المراقبة الأمنية طريقة تستخدم لتأكيد فاعلية والامتثال للممارسات والضوابط الأمنية السائدة. وتتشكل المراقبة من الأنشطة مثل مراجعة:

- سجلات أنظمة كشف التسلل المحوسبة
- سجلات جدار الحماية
- سجلات حساب المستخدم
- سجلات تحديد نشاط الحواسيب المضيفة على الشبكة
- سجلات التطبيق
- سجلات استرداد النسخ الاحتياطية للبيانات
- سجلات مكتب المساعدة
- السجل الأخر وملفات الخطأ

الغرض

إن غرض سياسة المراقبة الأمنية هي ضمان تطبيق سريان أمن مصادر المعلومات وعدم تجاوزها أحدى مزايا المراقبة الأمنية هي التعريف المبكر للمخالفات والثغرات الأمنية. يمكن أن يساعد التعريف المبكر في منع المخالفة والثغرات الأمنية قبل إلحاق الضرر أو على الأقل لخفض الأثر المحتمل. تتضمن المزايا الأخرى الامتثال للتدقيق ومراقبة مستوى الخدمة وقياس الأداء والمسؤولية المحدودة وتخطيط القدرة.

الجمهور

تنطبق سياسة المراقبة الأمنية بمؤسسة عيد الخيرية على جميع الأفراد المسؤولين عن تثبيت مصادر المعلومات الجديدة وعمليات موارد المعلومات الحالية والأفراد المسؤولين عن أمن مصادر المعلومات.

تعاريف

مصادر المعلومات (IR): أي من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

موظف أمن المعلومات : مسؤول عن إدارة مهام أمن المعلومات داخل المؤسسة. وهو نقطة الاتصال الداخلية والخارجية لجميع المسائل المتصلة بأمن معلومات المؤسسة.

الشبكة المحلية شبكة الاتصال بالبيانات لنطاق جغرافي محدد لبضعة أميال بحد أقصى. تقدم الشبكة الاتصال بين الحواسيب والأجهزة الملحقة في معدلات مرتفعة نسبيًا ومعدلات خطأ قليلة.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية
		2017/01/01	- منقحة
سياسة **المراقبة الأمنية**		نظم المعلومات	-المحرر

سياسة المراقبة الأمنية

- يتم مراقبة النظم الداخلية الخاصة بالمؤسسة من خلال بعض البرامج والتي تسهل عملية كشف المخالفات والتي تساعد على تحديث السياسات الأمنية المعمول بها ، ويتم استخدام هذه البرامج لمراقبة:
  - الشبكة.
  - البريد الإلكتروني.
  - نظام التشغيل.

- فحص الملفات الآتية بشكل دوري:
  - خطر الإصابة للفيروسات على مستوى الخوادم وأجهزة المستخدمين.
  - حسابات المستخدمين
  - أخطاء أنظمة التشغيل
  - النسخ الاحتياطية للبيانات والاسترداد
  - طلبات المستخدمين
  - نشاط الهاتف- تقارير تفاصيل الاتصال.
  - البريد الإلكتروني

- يتم إجراء الاختبارات التالية سنويًا على الأقل عن طريق الأفراد المعينين:
  - قوة كلمة السر
  - إعادة استخدام النسخ الاحتياطية.
  - تراخيص البرمجيات.
  - الثغرات الأمنية.

- يتم الإبلاغ عن أي أمور أمنية معلوماتية إلى إدارة نظم المعلومات.

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع المخلف.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	- سارية
		2017/01/01	- منقحة
سياسة **المراقبة الأمنية**		نظم المعلومات	-المحرر

معلومات الدعم **يتم دعم السياسة الأمنية بواسطة معايير السياسة الأمنية التالية**

مرجع #	تفاصيل معايير السياسة
5	يجب مراجعة صلاحيات وصول المستخدمين بصفة دورية إلى مصادر المعلومات بما في ذلك التغييرات التي قد تحدث على الموظفين مثل التنقل أو الترقية أو خفض المنصب أو الدرجة أو إنهاء الخدمة.
6	استخدام مصادر المعلومات لأغراض الأعمال المصرح بها رسميا فقط. لا يوجد ضمان للخصوصية الشخصية أو الوصول إلى أدوات والتي تتضمن على سبيل المثال لا الحصر، البريد الإلكتروني وتصفح الويب وأدوات المناقشة الإلكترونية الأخرى. قد يتم رصد استخدام أدوات التواصل الإلكتروني للوفاء بمتطلبات الشكوى أو التواصل مع المتبعرين والكفلاء .
16	رئيس قسم البنية التحتية والشبكات مسؤول عن تحديد صلاحيات الوصول إلى البرمجيات وأماكن تخزين البيانات المختلفة طبقاً لاحتياجات كل إدارة.
17	تقييم جميع الإدارات بدقة لمخاطر التعديل غير المصرح به أو الإفشاء غير المصرح به أو فقدان البيانات التي تقع ضمن مسؤوليتهم وتضمن من خلال استخدام نظم الرصد حماية مؤسسة عيد الخيرية من الضرر أو المخاطر النقدية أو خلاف ذلك. تحتفظ إدارات المالك وأمين الحفظ بالنسخ الاحتياطية وخطط الطوارئ المناسبة للتعافي من الكوارث استناداً إلى متطلبات تقييم المخاطر والأعمال.

إدارة نظم المعلومات	سياسة أمن مصادر المعلومات	2012/01/01	- سارية
		2017/01/01	-منقحة
سياسة **الوعي الأمني**		نظم المعلومات	-المحرر

مقدمة

فهم أن أهمية أمن الحاسوب والمسؤوليات الفردية والمسؤولية عن أمن الحاسوب مشروط بتحقيق أهداف أمن المنظمة. يمكن تحقيق هذا من خلال دمج تدريب الوعي العام بأمن الحاسوب والتدريب المستهدف والتدريب الخاص بالمنتج. يتطلب تدريس فلسفة الحماية والتدريبات الخاصة بالأمن إلى تعزيزها مع مستخدمي الحاسوب. يتطلب تحسين وتعزيز الوعي بالأمن ومعلومات التدريب باستمرار.

الغرض

إن غرض سياسة التدريب الأمني هو وصف المتطلبات لضمان استلام كل مستخدم في مؤسسة عيد الخيرية للتدريب الملائم على الأمور الأمنية للحاسوب.

الجمهور

تطبق سياسة التدريب الأمني لمؤسسة عيد الخيرية بالتساوي على جميع الأفراد المستخدمين لمصادر معلومات عيد الخيرية.

تعاريف

مصادر المعلومات (IR): أي من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

إدارة نظم المعلومات : اسم الإدارة المسؤولة عن الحواسيب والشبكة وإدارة البيانات.

إدارة نظم المعلومات	سياسة أمن مصادر المعلومات	2012/01/01	- سارية
		2017/01/01	-منقحة
سياسة **الوعي الأمني**		نظم المعلومات	-المحرر

سياسة الوعي الأمني

- يجب أن يطلع جميع مستخدمي مؤسسة عيد الخيرية على السياسات الأمنية للحاسوب .
- يجب أن ترسل إدارة نظم المعلومات رسائل توعويه لأمن المعلومات التي تصف بدقة السياسات والإجراءات الأمنية لمؤسسة عيد الخيرية.
- يجب أن ترسل إدارة نظم المعلومات بصفة دوية نشرة بريدية تظهر مخاطر الاختراقات الأمنية على الفرد والمؤسسة.
- يجب على كل موظف من موظفي مؤسسة عيج الخيرية الإبلاغ عن أي ثغرات أمنية يتم اكتشافها إلى المسؤول المباشر أو مدير إدارة نظم المعلومات.

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع المظف.

إدارة نظم المعلومات	سياسة أمن مصادر المعلومات	2012/01/01	- سارية
		2017/01/01	-منقحة
سياسة **الوعي الأمني**		نظم المعلومات	-المحرر

دعم المعلومات	تُدعم سياسة الأمن هذه بواسطة معايير سياسة الأمن الآتية.

مرجع #	تفاصيل معايير السياسة
2	يجب تأكيد وتعزيز وتحديث والمصادقة باستمرار على الوعي الأمني للعاملين.
3	يتحمل جميع العاملين مسؤولية إدارة استخدام مصادر المعلومات ويخضعوا للمساءلة عن أفعالهم المتعلقة بأمن مصادر المعلومات كما يتحمل العاملون أيضا على حد سواء مسؤولية الإبلاغ عن أي انتهاكات مشتبه فيها أو مؤكدة لهذه السياسة إلى الإدارة المختصة.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	-سارية
		2017/01/01	-تم مراجعتها
سياسة تطوير النظام		نظم المعلومات	-المحرر

مقدمة

يواصل عدد الحوادث الأمنية والتكلفة الناتجة عن توقف العمل وإعادة الخدمة في التصاعد. ويعد تطبيق سياسات الأمن المشدد ومنع وصول الشبكات والحواسيب الغير ضرورية وتحسين الوعي الأمني لدى المستخدم والكشف المبكر عن الحوادث الأمنية والتخفيف من آثارها كبعض الإجراءات التي يمكن اتخاذها للحد من المخاطر وخفض التكلفة الناجمة عن الحوادث الأمنية.

الغرض

الغرض من "سياسة تطوير النظام" هو وصف متطلبات التطوير و/أو تطبيق نظام برمجي جديد لمؤسسة عيد الخيرية.

الجمهور

تُطبق سياسة تطوير النظام لمؤسسة عيد الخيرية بالتساوي على جميع الأفراد المستخدمين لمصادر معلومات عيد الخيرية.

تعاريف

مصادر المعلومات (IR): أي من أو جميع مطبوعات الحاسوب وأجهزة العرض على الإنترنت ووسائط التخزين المغناطيسية وجميع الأنشطة المتصلة بالحاسوب التي تنطوي على أي جهاز قادر على تلقي البريد الإلكتروني وتصفح مواقع الإنترنت، أو خلاف ذلك أي جهاز قادر على استلام وتخزين وإدارة أو نقل البيانات الإلكترونية بما في ذلك، ولكن لا يقتصر على الحاسوب المركزي والخوادم والحاسوب الشخصي وأجهزة الحاسوب المحمولة وأجهزة الحاسوب المحمولة ومصادر الاتصالات السلكية واللاسلكية وبيئات الشبكة والهواتف وأجهزة الفاكس والطابعات ومكاتب الخدمات. بالإضافة إلى ذلك، فهي الإجراءات والمعدات والمرافق والبرمجيات والبيانات التي تم تصميمها وبنائها وتشغيلها وحفظها لإنشاء وجمع وتسجيل ومعالجة وتخزين واسترداد وعرض ونقل المعلومات.

تعاريف، تابع

دورة حياة تطوير النظم: هي مجموعة من الإجراءات لتوجيه تطوير إنتاج برمجيات التطبيقات وعناصر البيانات. وتشمل دورة حياة تطوير النظم النموذجية على التصميم والتطوير والصيانة وضمان الجودة واختبار القبول.

المستخدم: يقع في مسؤوليته: (1) استخدام المعلومات فقط للغرض المحدد من قبل المؤسسة (2) الامتثال للضوابط التي وضعتها المؤسسة (3) منع الكشف عن المعلومات الخاصة بالمؤسسة . والمستخدم هو أي شخص مصرح له بقراءة أو إدخال أو تحديث المعلومات. والمستخدم هو عنصر التحكم الفردي الأكثر فعالية لتوفير الأمن الكافي.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	-سارية
		2017/01/01	-تم مراجعتها
سياسة تطوير النظام		نظم المعلومات	-المحرر

سياسة تطوير النظام

- يقع على إدارة نظم المعلومات مسؤولية التطوير والصيانة والمشاركة في دورة حياة تطوير البرمجيات بمشروعات تطوير النظم لمؤسسة عيد الخيرية. يتعين على إدارة نظم المعلومات وضع خطة تطوير جميع البرمجيات التي تم برمجتها داخلياً أو عن طريق مزودي الخدمات . وكحد أدنى، ينبغي أن تتناول هذه الخطة مجالات التحليل الأولى أو دراسة الجدوى وتحديد المخاطر والتخفيف من آثارها وتحليل النظم والتصميم العام والتطوير وضمان الجودة واختبار القبول والتطبيق وصيانة ما بعد التطبيق. وتضمن هذه المنهجية أنه سيتم توثيق البرامج على نحو كاف واختبارها قبل استخدامها للمعلومات الهامة لمؤسسة عيد الخيرية.
- يجب وضع البرمجيات الجديدة على خادم لاختبارها من قبل المستخدمين قبل تفعيلها.
- يجب أن يتم تدريب المستخدمين المعنيين على النظم الجديدة أو الميزات الإضافية التي تم إضافتها للبرامج المحدثة
- يجب التنبيه من قبل إدارة نظم المعلومات على وجود تحديثات جديدة في النظم لجميع المستخدمين.

الإجراءات التأديبية

قد يؤدي انتهاك هذه السياسة إلى إجراءات تأديبية قد تشمل إنهاء الخدمة للموظفين والوقف المؤقت أو الإنذار أو أي عقوبات أخرى تحددها لجنة التحقيق مع الموظف

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	ـسارية
		2017/01/01	ـتم مراجعتها
سياسة تطوير النظام		نظم المعلومات	ـالمحرر

معلومات الدعم **يتم دعم السياسة الأمنية بواسطة معايير السياسة الأمنية التالية**

مرجع #	تفاصيل معايير السياسة
8	يجب حماية جميع برمجيات الحاسوب والتطبيقات والتعليمات البرمجية المصدر والوثائق والبيانات وتكون من مسؤولية رئيس قسم البنية التحتية والشبكات.
10	يتعين على طالب الخدمة في بداية أي مشروع أن يقوم بإشراك مدير مصادر المعلومات أو شخص مُكلف للحصول على أجهزة كمبيوتر أو شراء أو تطوير برامج الكمبيوتر. ويجب أن يتم الموافقة على تكاليف الشراء وتشغيل أجهزة الحاسوب والتطبيقات بواسطة إدارة مناسبة. وعلى الإدارة الطالبة أن يعملوا في إطار حدودهما المخولة إليهما والموافق عليها وفقا لنهج التخويل الخاص بالمؤسسة .
11	يجب أن تتخذ الإدارة التي تطلب وتصرح بأحد تطبيقات الحاسوب الخطوات المناسبة لضمان سلامة وأمن جميع البرامج وملفات البيانات التي تم إنشاؤها.
14	سلامة استخدام البرمجيات والأجهزة، ونظم التشغيل والشبكات وملفات البيانات العامة هي مسؤولية رئيس قسم البنية التحتية والشبكات.
17	تقييم جميع الإدارات بدقة لمخاطر التعديل غير المصرح به أو الإفشاء غير المصرح به أو فقدان البيانات التي تقع ضمن مسؤوليتهم وتضمن من خلال استخدام نظم الرصد حماية مؤسسة عيد الخيرية من الضرر أو المخاطر النقدية أو خلاف ذلك. تحتفظ إدارات المالك وأمين الحفظ بالنسخ الاحتياطية وخطط الطوارئ المناسبة للتعافي من الكوارث استناداً إلى متطلبات تقييم المخاطر والأعمال.

إدارة نظم المعلومات	سياسات أمن نظم المعلومات	2012/01/01	-سارية
		2017/01/01	-تم مراجعتها
سياسة تطوير النظام		نظم المعلومات	-المحرر