عيوني
Oyouny

سياسة استخدام التقنية

وأمن المعلومات

عيوني
Oyouny
جمعية عيوني الصحية

0546684628 Oyouny.sa Oyouny_sa

أولاً: سياسات عامة:

1. يصرح لمستخدمي الموارد المعلوماتية في الجمعية باستخدامها لأغراض تخص العمل فقط, ولا يجوز استخدامها لأغراض تخالف الأنظمة واللوائح المعمول بها في المملكة, أو بما يؤدي إلى الإضرار بالجمعية أو بسمعتها, ويشمل ذلك منع استخدام الموارد المعلوماتية للأغراض التالية:

- استخدامها في أي عمل أو غرض غير شرعي.
- استخدامها بما يتعارض مع الأخلاق والآداب العامة.
- انتحال شخصية شخص أو جهاز آخر.
- التعامل باسم الجمعية أو أي من أقسامها أو أي من موظفيها دون إذن كتابي رسمي.
- نشر المعلومات الشخصية أو الخاصة بالآخرين دون إذن صريح بذلك.
- محاولة فك تشفير بيانات الآخرين في الأنظمة المعلوماتية.
- الإخلال بأي من حقوق النشر أو التأليف, أو حقوق الملكية الفكرية لأي بيانات أو معلومات.
- مراقبة الاتصالات الإلكترونية للمستخدمين الآخرين (التجسس).
- الاستخدام بشكل يؤثر سلبياً على المستخدمين الآخرين, أو على أداء الأجهزة والشبكات.
- الاستخدام الذي يمكن أن يتسبب في أي تهديد, أو تخريب, أو إزعاج, أو إهانة, أو مضايقة لأي شخص أو جهة أو أمنها الإلكتروني مثل إرسال بريد إلكتروني بشكل متكرر, أو غير مرغوب فيه, أو لغرض الغش, أو الخداع الآخرين.
- إنشاء موقع الكتروني يمثل الجمعية, أو إدارته, دون إذن كتابي رسمي من صاحب الصلاحية.
- عدم استخدام قنوات اتصال بالموارد المعلوماتية للجمعية أو الارتباط بها, إلا من خلال القنوات المتاحة والمصرح بها رسمياً من إدارة الجمعية.
- استخدام الموارد المعلوماتية بشكل يؤدي إلى إهدار وقت الموظف.

2. يعتبر المستخدم مسؤولاً مسؤولية كاملة عن كل ما يصدر من استخدام لجهازه أو من خلال الحساب الخاص به, وعليه الحرص على أمن الدخول للموارد المعلوماتية المنوطة به.
3. تعد المراسلات عن طريق البريد الإلكتروني الخاص بالجمعية ملكاً للجمعية ويحق الاطلاع على تلك المراسلات في حالة وجود تحقيق رسمي.
4. على المستخدم التوقيع على قبول سياسة أمن المعلومات في الجمعية قبل السماح له باستخدام الموارد المعلوماتية.
5. إغلاق أجهزة الحاسب بعد نهاية الدوام حفاظاً عليها وترشيداً للاستخدام.
6. عدم تثبيت أي برامج ضارة أو تجسسيه في الأجهزة الشخصية مالم سيتحمل الموظف المسئولية الكاملة عن ذلك أمام إدارة الجمعية.

ثانياً: سياسة التحكم في الوصول للبيانات والمعلومات

الهدف

ضمان تطبيق الجمعية لعملية التحكم في الوصول إلى المعلومات الإلكترونية المتعلقة بالجمعية, وضمان توافقها مع المتطلبات القانونية والأمنية حيثما تقتضي الحاجة.

مجال التطبيق

تنطبق هذه السياسة على جميع موظفي وأعضاء ومتطوعي الجمعية وأي جهة ترتبط بأي شكل بمرافق نظم المعلومات بالجمعية.

السياسة

1. الالتزام بسياسة التحكم في الوصول للمعلومات في الجمعية يقلل فرص التعرض للخروقات الأمنية في الوقت الذي يسمح لإدارة تقنية المعلومات بأن يقوموا بأنشطتهم في إطار السياسات.
2. يقتصر التحكم في الوصول لمعلومات وبيانات الجمعية على المستخدمين المسموح لهم فقط وذلك لمنع تعرض التطبيقات أو البيانات والمعلومات لأي خرق أو تعديل عرضي أو غير مقصود.
3. تتحكم إجراءات تسجيل هوية المستخدم في منح صلاحية الدخول للحسابات أو وقفها أو حذفها.
4. يتم إنشاء وتفعيل حسابات مستخدمي الجمعية أو المتطوعين بواسطة وحدة تقنية المعلومات في الجمعية.
5. يمنح المستخدمون امتيازات مع حساباتهم حسب ما يتناسب ودورهم ووظيفتهم على وجه الخصوص.
6. يتم التحكم باستخدام أو منح كلمة المرور وفق سياسة كلمة المرور.
7. يجب حماية كافة أجهزة الحاسب التي تنتمي للشبكة بكلمة مرور وشاشة توقف معيارية.
8. يجب على المستخدمون إيقاف أجهزتهم النشطة التي لا يعملون عليها.
9. مسؤولية ترك أجهزة الحاسب غير مستخدمة تقع على عاتق المستخدمين.
10. أفضل طريقة للقفل التلقائي لشاشة التوقف هي أن يضبط المؤقت على 15دقيقة بحيث يتم توفير الأمن الضروري في الوقت الذي لا يتسبب ذلك في إزعاج المستخدم.
11. يجب الالتزام بمعايير اختيار كلمات المرور كما هو مدرج في سياسة كلمة المرور.

ثالثاً: سياسة النسخ الاحتياطية واستعادة وحفظ البيانات

الهدف

الهدف من هذه السياسة هو توضيح قواعد عمل نسخة احتياطية من بيانات الجمعية لضمان إمكانية استردادها.

مجال التطبيق

تنطبق هذه السياسة على جميع موظفي وأعضاء ومتطوعي الجمعية

السياسة

1. وحدة تقنية المعلومات هي المسؤولة عن عملية استرداد المعلومات / البيانات الإلكترونية في حال تلف البيانات.
2. يجب أن تضمن وحدة تقنية المعلومات الترتيبات اللازمة لاستئناف العمل في الجمعية بصورة عادية في فترة معقولة من الوقت, مع فقدان الحد الأدنى من البيانات. ونظراً لاحتمالات أن تتعطل الأنظمة لأسباب عديدة مع مرور الزمن, فينبغي الحفاظ على أجيال متعددة من النسخ الاحتياطية لضمان استمرارية الخدمات الهامة.
3. جميع النسخ الاحتياطية لمعلومات وبيانات الجمعية يجب أن يتم حفظها وأن تكون قابلة للاسترداد بشكل كامل.
4. يجب الحفاظ على ثلاث نسخ احتياطية من معلومات وبيانات الجمعية كحد أدنى.
5. يجب الاحتفاظ بنسخة احتياطية كاملة لمعلومات وبيانات الجمعية في بيئة آمنة وخارج مقر الجمعية.
6. يتم فقط حفظ معلومات وبيانات الجمعية الموجودة على خادم الشبكة ويتم دعمها وفقاً لإجراءات حفظ النسخ الاحتياطية بالجمعية.
7. إجراءات استعادة البيانات يجب تحديثها والتحقق منها بشكل دوري.

رابعاً: سياسة أمن المعلومات

الهدف

1. تأمين الحماية لبيانات الجمعية من التداعيات المحتملة الناتجة عن خروقات السرية أو الأضرار الفيروسية.
2. ضمان حماية كافة أصول المعلومات ومرافق الشبكات والحواسيب من التلف أو الفقدان أو سوء الاستخدام.
3. ضمان معرفة موظفي وأعضاء الجمعية والمتطوعين بمبادئ استخدام المعلومات الإلكترونية والالتزام بها.
4. زيادة مستوى الوعي والفهم تجاه متطلبات أمن المعلومات في الجمعية وسرية وسلامة البيانات التي يمتلكونها أو يتعاملون بها.

مجال التطبيق

تطبق هذه السياسة على أنواع الأمن التالية بالجمعية:

أ- تنطبق هذه السياسة على جميع موظفي وأعضاء ومتطوعي الجمعية.

ب- تنطبق هذه السياسة على بيانات الجمعية وبرامجها وأنظمتها وأجهزة الحاسب والشبكات السلكية واللاسلكية.

السياسة

1. يجب حماية المعلومات من أي اختراق غير مسموح به.
2. يلتزم جميع العاملين في الجمعية والمتطوعين بسرية المعلومات والحفاظ على خصوصيتها.
3. يلتزم جميع العاملين في الجمعية والمتطوعين بالحفاظ على سلامة ومصداقية المعلومات.
4. يلتزم جميع العاملين في الجمعية والمتطوعين بالحفاظ على إتاحة المعلومات.

5. إبلاغ "وحدة تقنية المعلومات" عن كافة أشكال الخروقات الفعلية أو المحتملة لأمن المعلومات من أجل القيام بالإجراء اللازم.
6. تحديث جميع برمجيات مكافحة الفيروسات من قبل خدمات تقنية المعلومات بانتظام, مع التحقق من الأنظمة.
7. التحقق من أن جميع الملفات التي تم تحميلها عن طريق البريد الإلكتروني خالية من الفيروسات.
8. التأكد من أن جميع السيرفرات قد تم تزويدها ببرامج مكافحة الفيروسات وأن كفاءتها ضد الفيروسات مضمونة.
9. التحقق من فحص جميع الوسائط من الفيروسات قبل الاستخدام من قبل المستخدم.
10. يُسمح لأي مستخدم باستخدام الوسائط في أجهزة الحواسيب المكتبية الخاصة به, بعد التحقق من خلوها من الفيروسات.
11. يجب أن يتم فحص جميع مراسلات البريد الإلكتروني الصادر والوارد للتأكد من خلوها من الفيروسات والمحتوى الضار قبل فتحها وخاصة مرفقات البريد الإلكتروني.
12. لن يحصل المستخدم على أي تفويض إداري في تفعيل أو تعطيل ميزات برنامج مكافحة الفيروسات.
13. يتم قفل حساب المستخدم المتضرر وفصل النظام المتضرر في الشبكة وعزله وتطويقه الى أن يتم تطهيره من قبل وحدة تقنية المعلومات.
14. يلتزم جميع العاملين في الجمعية والمتطوعين بعدم الوصول للبريد الإلكتروني ذو المحتوى الضار أو المشكوك فيه من قبل المستخدمين دون تعليمات من قبل وحدة تقنية المعلومات.

خامساً: سياسة كلمة المرور

الهدف

تحمي سياسة إدارة كلمات المرور الفعالة بيانات الجمعية وتخفض من مخاطر الدخول غير المسموح به, وتهدف هذه السياسة إلى إنشاء بيئة آمنة لتقنية معلومات من خلال تفعيل استخدام كلمات المرور القوية.

مجال التطبيق

تُطبق هذه السياسة على جميع العاملين الذين لديهم, أو هم مسؤولين عن, حسابات أو أي شكل من أشكال الدخول الذي يتطلب كلمة مرور. ويشمل ذلك أي نظام متواجد بالجمعية أو يتمتع بحق الدخول إلى الشبكة أو يخزن معلومات ليست متاحة للعامة عن الجمعية.

السياسة

1. يجب ان يلتزم الموظفين بالإرشادات أدناه لإنشاء كلمة مرور قوية:
   - كلمات المرور القوية تملك تشكيلة الأحرف التالية :
   - تحوي كلا من الأحرف الكبيرة والصغيرة , مثلا. (a-z, A-Z)
   - تحوي أرقاما وعلامات ترقيم بالإضافة إلى الأحرف, مثلا: @ , $,#, &
   - طولها على الأقل ثمانية أحرف وأرقام.
   - غير مبنية على المعلومات الشخصية كاسم العائلة ...الخ
   - يجب عدم كتابة كلمة المرور أو تخزينها على الشبكة.
2. يجب أن يلتزم الموظفون بالتعليمات التالية في التعامل مع كلمة المرور:
   - لا تكشف كلمة المرور عبر الهاتف لأي أحد.
   - لا تكشف كلمة المرور في رسالة الكترونية.

- لا تتحدث عن كلمة المرور أمام الآخرين.
- لا تقتبس تشكيلة كلمة المرور من أسماء خاصة بك مثل اسم العائلة أو تاريخ الميلاد.
- لا تكشف كلمة المرور في نماذج الاستفتاءات الأمنية.
- لا تكشف كلمة المرور لزملاء العمل.

3. يجب التعامل مع كلمات المرور كافة بوصفها معلومات حساسة وسرية في الجمعية.
4. تُفعل سياسة كلمة المرور بشكل تلقائي.
5. تقع على عاتق جميع أعضاء الجمعية مسؤولية اختيار كلمات مرورهم بشكل آمن بحيث تتوافق مع المعايير التالية:

الوصف	الضبط	الضبط المعرف الخاص بالمستخدم
الطول الأدنى لكلمة المرور	8	8
الفترة القصوى لكلمة المرور بالأيام	تتراوح مدة الفترة الزمنية بين يوم و 90يوم وتعني القيمة "صفر" أن كلمة المرور لن تنتهي صلاحيتها على الإطلاق.	90 يوماً
تاريخ كلمة المرور	يحدد ذلك احتمالية استخدام كلمات المرور القديمة مجدداً, ويمثل ذلك الرقم عدد كلمات المرور الجديدة اللازم استخدامها قبل إعادة استخدام كلمة مرور قديمة	60 يوماً
درجة تعقيد كلمة المرور	يجب أن تحتوي كلمة السر على الفئات التالية: • أحرف كبيرة باللغة الإنجليزية مثل A, B, C, ... Z • أحرف صغيرة باللغة الإنجليزية مثل a,b,c • رموز خاصة مثل @*^#% !()":., • الأرقام مثل 1 ,2,3	مفعلة

سياسة البريد الإلكتروني

الهدف

تهدف هذه السياسة لضمان الاستخدام الأمثل والآمن لخدمة البريد الإلكتروني من قبل موظفي وأعضاء ومتطوعي الجمعية.

مجال التطبيق

تنطبق هذه السياسة على جميع موظفي وأعضاء ومتطوعي الجمعية وأي جهة ترتبط بأي شكل بمرافق نظم المعلومات بالجمعية.

السياسة

1. يجب على المستخدمين استخدام خدمات البريد الإلكتروني الرسمي للجمعية في المعاملات الرسمية, وعدم استخدام خدمات البريد الإلكتروني الشخصي.
2. على المستخدم الحذر عند اعادة توجيه أي بريد إلكتروني, وعدم توجيه كلاً من البريد الإلكتروني غير المرغوب فيه والإعلانات التجارية والبريد العشوائي.
3. يُسمح فقط للمستخدمين بإرسال رسائل البريد الإلكتروني والمرفقات التي تتفق مع القيم الدينية والثقافية والسياسية والأخلاقية للدولة, مع عدم السماح بإرسال رسائل قد تسبب ضرراً للجمعية أو تؤدي إلى تشويه صورتها وسمعتها.
4. لا يُسمح للمستخدمين بإرسال أو الرد أو توجيه رسائل البريد الإلكتروني ذو المحتوى السري أو التي تنتهك حقوق الملكية الفكرية.
5. يحظر على المستخدمين ارسال أو الرد أو توجيه رسائل البريد الإلكتروني التي تحتوي على مرفقات مصابة بالفيروسات أو أي برمجيات ضارة.
6. على المستخدمين عدم فتح رسائل البريد الإلكتروني غير المرغوب فيها, مع حذفها من النظام.
7. يحظر على المستخدمين استخدام البريد الإلكتروني للجمعية في المعاملات الخاصة.

8. يحظر على المستخدمين استخدام نظام البريد الإلكتروني للجمعية لانتحال صفة شخص آخر.
9. على المستخدمين التحقق والتأكد من أن مرفقات رسائل البريد الإلكتروني خالية من الفيروسات أو أي تعليمات برمجية ضارة.
10. على المستخدمين استخدام التواقيع وإخلاء المسؤولية المعتمدة في الجمعية مع كافة رسائل البريد الإلكتروني.
11. على المستخدمين عدم تسجيل عنوان البريد الإلكتروني الخاص بالجمعية في المواقع الالكترونية لغير أغراض العمل.

وقد تم اعتماد هذه اللائحة
في اجتماع مجلس الإدارة الثالث

في دورته الأولى بتاريخ 2021/10/12م