جمعية البر الخيرية بالحكامية بجازان

مسجلة بالمركز الوطني لتنمية القطاع غير الربحي برقم (457)

سياسة
تقنية المعلومات

الإصدار الأول

2023م

نظرة عامة

تحدد هذه السياسة الآليات المتبعة لتأمين بيانات ومعلومات أصحاب المصلحة والتأكيد على سريتها والحفاظ على أنظمة تكنولوجيا المعلومات والبنية التحتية ضد المخاطر الأمنية.

مجال التطبيق

تطبق هذه السياسة على أنواع الأمن التالية بالجمعية :

(1)أمن تطبيقات ونظم الحاسب
(2)الأمن المادي
(3)الأمن التشغيلي
(4)الأمن الإجرائي
(5)أمن الشبكات

الهدف

(1)تأمين الحماية من التداعيات المحتملة الناتجة عن خروقات السرية أو انقطاعات الخدمة المتاحة.
(2)ضمان حماية كافة أصول المعلومات ومرافق الشبكات والحوسبة من التلف أو الفقدان أو سوء الاستخدام.
(3)ضمان معرفة أعضاء الجمعية بمبادئ استخدام المعلومات الإلكترونية والالتزام بها.
(4)زيادة مستوى الوعي والفهم تجاه متطلبات أمن المعلومات في الجمعية .
(5)زيادة الوعي من جانب المستخدمين تجاه مسؤولياتهم المباشرة عن حماية سرية وسلامة البيانات التي يمتلكونها أو يتعاملون بها.

السياسة

(1)تعتمد الجمعية على إتاحة وسلامة خدماتها الالكترونية في مراحل تسجيل المستفيدين والتواصل عن بعد . وفي إطار ذلك يكون من الضروري حماية نظم تقنية المعلومات والبنى التحتية من مخاطر أمنية سواء أكانت داخلية أو خارجية أو متعمدة أو عرضية.
(2)يتوجب على جميع العاملين والمتعاملين مع الجمعية الالتزام بمعرفة الآليات واللوائح التي تضمن ما يلي:

أ)حماية المعلومات من أي اختراق غير مسموح به.
ب)سرية المعلومات.
ج)الحفاظ على سلامة ومصداقية المعلومات.
د)الحفاظ على إتاحة المعلومات.
ه)تحقيق المتطلبات التنظيمية والتشريعية.
و)إتاحة التدريب والمعرفة بأمن المعلومات بالنسبة لأعضاء الجمعية .
ز)إبلاغ" قطاع تقنية المعلومات "عن كافة أشكال الخروقات الفعلية أو المحتملة لأمن المعلومات من أجل القيام بالإجراء اللازم.
ح)إيجاد إجراءات من شأنها دعم هذه السياسة بما في ذلك إجراءات ضبط الفيروسات وكلمات المرور وخطط الاستمرارية.
ط)تحقيق متطلبات إتاحة النظم والمعلومات.
ي)عدم السماح لأي نوع من النظم الاتصال بالشبكة دون برنامج مكافحة الفيروسات.

(ك) تحديث جميع مكونات النظام والبرمجيات من قبل خدمات تقنية المعلومات بانتظام، مع التحقق من الأنظمة.

(ل) التحقق من أن جميع الملفات التي تم تحميلها عن طريق البريد الإلكتروني خالية من الفيروسات.

(م) التأكد من أن جميع الخوادم قد تم تزويدها ببرامج مكافحة الفيروسات وأن كفاءتها ضد الفيروسات مضمونة.

(ن) يتم فحص جميع الوسائط غير المثبتة والمسح الضوئي للفيروسات قبل استخدامها من قبل المستخدم.

(3) يسمح لأي مستخدم باستخدام شريحة ذاكرة في أجهزة الحواسيب المكتبية الخاصة به، بعد التحقق من خلوها من الفيروسات.

(4)يتم مسح جميع مراسلات البريد الإلكتروني الصادر والوارد للتأكد من خلوها من الفيروسات والمحتويات الضارة) .

(5) يتم تحديث خادم البريد بشكل دوري بأحدث برامج (service packs/ patches) لمكافحة الفيروسات.

(6) يتم عزل رسائل البريد الإلكتروني المصابة والاحتفاظ بها في نظام العزل مع إخطار المستخدم، وتقديم الحل المناسب من خدمات تقنية المعلومات.

(7) لن يحصل المستخدم على أي تفويض إداري في تفعيل أو تعطيل ميزات برنامج مكافحة الفيروسات.

(8) يتم إغلاق حساب المستخدم المتضرر وفصل النظام المتضرر من الشبكة وعزله الى أن يتم تطهيره من قبل قطاع تقنية المعلومات.

(9) لن يتم الوصول للبريد الإلكتروني ذو المحتوى الضار أو المشكوك فيه من قبل المستخدم دون تعليمات من قبل قطاع تقنية المعلومات.

(10) على جميع الحواسيب العاملة والمتصلة بشبكة الجمعية أن تكون ضمن المجال الخاص بالجمعية على شبكة الانترنت.

(11) يعتبر" قطاع تقنية المعلومات "مسؤولا عن الحفاظ على هذه السياسة وعن تقديم الدعم والنصيحة أثناء تنفيذها.

إجراءات السياسة رقم (6) - أمن المعلومات

1- السرية والخصوصية

يتحتم على جميع أعضاء الجمعية احترام وحماية خصوصية البيانات .وبينما لا تراقب الجمعية محتوى صفحات المواقع الشخصية أو البريد الإلكتروني أو أية وسائل أخرى للتواصل الإلكتروني إلا أن للجمعية الحق في معاينة سجلات الحواسيب أو في مراقبة أنشطة الحواسيب الشخصية وذلك بموافقة إدارة الجمعية.

2- الولوج

لا يجوز لأحد في الجمعية الدخول إلى السجلات الخاصة إلا إذا كان مفوضاً بذلك على وجه التحديد، ويجوز للأشخاص المفوضين أن يستخدموا السجلات الخاصة لأسباب مشروعة فقط، ويجب الحفاظ على الممتلكات التكنولوجية في مكان آمن ومناسب، وينبغي على فريق الإدارة التأكد من وجود الضوابط اللازمة للحيلولة دون دخول غير المفوضين إلى النظم والشبكات وللكشف عن أي محاولات من هذا القبيل.

3- المسؤولية

يُعتبر جميع أعضاء الجمعية مسؤولين عن ضمان عدم استخدام الغير لامتيازاتهم وحقوقهم المتعلقة بنظام تقنية المعلومات، كما يعتبر الموظفون المخولون بالجمعية مسؤولين عن مراجعة سجلات الدخول وتحديد الخروقات الأمنية المحتملة .هذا ويجب أن تحتفظ كافة النظم المضبوطة بسجلات حتى يمكن متابعة استخدام المعلومات بدرجة مناسبة لكل نظام، كما يتعين على المسؤولين المخولين القيام بإخطار الإدارة فوراً في حالة الاشتباه في حدوث أية خروقات.

4- التوثيق

يتم تنفيذ التوثيق للاتصال من نقطة إلى نقطة لجميع النظم التي ترسل وتستقبل بيانات.

5- الإتاحة

يتوقع أن تكون نظم المهمات الحساسة متاحة في كل الأوقات .ويجب أن يكون هناك نظام حساس إضافي يتمتع بإجراءات استرداد المعلومات بشكل مفصل والإبلاغ عن الفترات التي تكون فيها النظم خارج الخدمة (أثناء عطل أو صيانة أو إصلاح)، كما ينبغي اختبار إجراءات النسخ الاحتياطية من البيانات وأن توثق بشكل جيد.

6- الإبلاغ عن الخروقات

تقع هذه المسؤولية على مالكي نظم التطبيقات والشبكات والحواسيب إضافة إلى مستخدمي هذه الأنظمة وتتمثل في الإبلاغ عن أية خروقات أمنية واضحة .ويجب أن تتاح الإرشادات الخاصة بالإبلاغ عن الخروقات لكل فرق الإدارة والمستخدمين، كما ينبغي أن تشتمل على إرشادات تتعلق بطبيعة هذه الخروقات والزمن والمكان والشخص والإطار الزمني الذي ينبغي من خلاله الإبلاغ عن هذه الخروقات.