جمعية البر الأهلية بالمجلاني

سياسة الحماية من البرمجيات الضارة

٢٠٢٠ م

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين)، في تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٩-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة الخاصة بجمعية البر الاهلية بالمحلاني وتنطبق على جميع العاملين في جمعية البر الاهلية بالمحلاني

بنود السياسة

١. البنود العامة

١-١ يجب تحديد متطلبات الأمن السيبراني المتعلقة بالعاملين.

١-٢ يجب أن يشغل الوظائف ذات العلاقة بالأنظمة الحساسة في جمعية البر الاهلية بالمحلاني مواطنين ذو الكفاءة اللازمة.

١-٣ يجب تنفيذ ضوابط الأمن السيبراني الخاصة بالموارد البشرية خلال دورة حياة عمل الموظف (Lifecycle) في جمعية البر الاهلية بالمحلاني والتي تشمل المراحل التالية:

- قبل التوظيف.
- خلال فترة العمل.
- عند انتهاء فترة العمل أو إنهائها.

٧. يجب توفير تقنيات الحماية اللازمة من الفيروسات، والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Protection) على خوادم البريد الإلكتروني؛ والتأكد من فحص الرسائل قبل وصولها لصندوق بريد المستخدم.

٨. يجب توثيق مجال البريد الإلكتروني جمعية البر الاهلية بالمحلاني عن طريق استخدام الوسائل اللازمة؛ مثل طريقة إطار سياسة المرسل (Sender Policy Framework) لمنع تزوير البريد الإلكتروني (Email Spoofing). كما يجب التأكد من موثوقية مجالات رسائل البريد الواردة (Incoming message DMARC verification).

٩. يجب أن يقتصر الوصول إلى رسائل البريد الإلكتروني على العاملين لدى جمعية البر الاهلية بالمحلاني

١٠. يجب اتخاذ الإجراءات اللازمة؛ لمنع استخدام البريد الإلكتروني بجمعية البر الاهلية بالمحلاني في غير أغراض العمل.

١١. يمنع وصول مسؤول النظام (System Administrator) إلى معلومات البريد الإلكتروني الخاصة بأي موظف دون الحصول على تصريح مسبق.

١٢. يجب تحديد حجم مرفقات البريد الإلكتروني الصادر والوارد، وسعة صندوق البريد لكل مستخدم وكذلك العمل على الحد من إتاحة إرسال الرسائل الجماعية لعدد كبير من المستخدمين.

١٣. يجب تذييل رسائل البريد الإلكتروني المرسلة إلى خارج جمعية البر الاهلية بالمحلاني بإشعار إخلاء المسؤولية.

١٤. يجب تطبيق التقنيات اللازمة؛ لحماية سرية رسائل البريد الإلكتروني وسلامتها، وتوافرها أثناء نقلها وحفظها؛ وتشمل هذه الإجراءات استخدام تقنيات التشفير وتقنيات منع تسريب البيانات.

١٥. يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لنظام البريد الإلكتروني.

١٦. يجب تعطيل خدمة تحويل البريد الإلكتروني من الخادم (Open Mail Relay).

٢-٨ يجب القيام بعمليات مسح دورية لأجهزة المستخدمين والخوادم والتأكد من سلامتها من البرمجيات الضارة.

٢-٩ يجب تحديث تقنيات الحماية من البرمجيات الضارة تلقائياً عند توفر إصدارات جديدة من المورد، مع الأخذ بالاعتبار سياسة إدارة التحديثات والإصلاحات.

٢-١٠ يجب توفير تقنيات حماية البريد الإلكتروني وتصفح الإنترنت من التهديدات المتقدمة المستمرة (APT Protection)، والتي تستخدم عادةً الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وتطبيقها وإداراتها بشكل آمن.

٢-١١ يجب ضبط إعدادات تقنيات الحماية بالسماح لقائمة محددة فقط من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج للعمل على الخوادم الخاصة بالأنظمة الحساسة. (CSCC-2-3-1-1)

٢-١٢ يجب حماية الخوادم الخاصة بالأنظمة الحساسة عن طريق تقنيات حماية الأجهزة الطرفية المعتمدة (End-point Protection). (CSCC-2-3-1-2) لدى جمعية البر الاهلية بالمحلاني

٢-١٣ يجب إعداد تقارير دورية حول حالة الحماية من البرمجيات الضارة يوضح فيها عدد الأجهزة والخوادم المرتبطة بتقنيات الحماية وحالتها (مثل: محدثة، أو غير محدثة، أو غير متصلة، إلخ)، ورفعها إلى مسؤول تقنية المعلومات.

٢-١٤ يجب إدارة تقنيات الحماية من البرمجيات الضارة مركزياً ومراقبتها باستمرار.

٣- متطلبات أخرى

٣-١ يجب على مسؤول تقنية المعلومات التأكد من توافر الوعي الأمني اللازم لدى جميع العاملين للتعامل مع البرمجيات الضارة والتقليل من خطورتها.

٣-٢ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية أجهزة المستخدمين والخوادم من البرمجيات الضارة.

٣-٣ يجب مراجعة متطلبات الأمن السيبراني لحماية أجهزة المستخدمين والخوادم الخاصة جمعية البر الاهلية بالمحلاني دورياً.

الأدوار والمسؤوليات

١. **راعي ومالك وثيقة السياسة:** مسؤول تقنية المعلومات.

٢. **مراجعة السياسة وتحديثها:** مسؤول تقنية المعلومات.

٣. **تنفيذ السياسة وتطبيقها:** المدير التنفيذي ومسؤول تقنية المعلومات.

الالتزام بالسياسة

١. يجب على مسؤول تقنية المعلومات ضمان التزام جمعية البر الاهلية بالمحلاني بهذه السياسة دورياً.

٢. يجب على كافة العاملين في جمعية البر الاهلية بالمحلاني الالتزام بهذه السياسة.

٣. قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية البر الاهلية بالمحلاني

جمعية البر الأهلية بالمحلاني

المحتويات