الموارد البشرية
والتنمية الاجتماعية

جمعية البر الخيرية في طلعة التمياط
Al - Bir Charity Association in Talat Al - Temyat

سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية

بجمعية البر خيرية في طلعة التمياط

المحتويات

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية الناتجة عن استخدام أجهزة المستخدمين (Workstations)، والأجهزة المحمولة (Mobile Devices)، والأجهزة الشخصية للعاملين (BYOD "Bring Your Own Device") داخل جمعية البر الخيرية بطلعة التمياط ، وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي سرية المعلومات وسلامتها وتوافرها.
تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة ، وهي متطلب تشريعي كما هو مذكور في الضوابط رقم 1-3-2 و1-6-2 من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية للعاملين داخل جمعية البر الخيرية بطلعة التمياط وتنطبق على جميع العاملين في جمعية البر الخيرية بطلعة التمياط .

بنود السياسة

1. البنود العامة

1-1 يجب حماية البيانات والمعلومات المُخزّنة في أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) حسب تصنيفها باستخدام الضوابط الأمنية المناسبة لتقييد الوصول إلى هذه المعلومات، ومنع العاملين غير المصرّح لهم من الوصول لها أو الاطلاع عليها.

1-2 يجب تحديث برمجيات أجهزة المستخدمين والأجهزة المحمولة، بما في ذلك أنظمة التشغيل والبرامج والتطبيقات، وتزويدها بأحدث حزم التحديثات والإصلاحات وذلك وفقاً لسياسة إدارة التحديثات والإصلاحات المعتمدة في جمعية البر الخيرية بطلعة التمياط .

1-3 يجب تطبيق ضوابط الإعدادات والتحصين (Configuration and Hardening) لأجهزة المستخدمين والأجهزة المحمولة وفقاً لمعايير الأمن السيبراني.
1-4 يجب عدم منح العاملين صلاحيات هامة وحساسة (Privileged Access) على أجهزة المستخدمين والأجهزة المحمولة، ويجب منح الصلاحيات وفقاً لمبدأ الحد الأدنى من الصلاحيات والامتيازات.
1-5 يجب حذف أو إعادة تسمية حسابات المستخدم الافتراضية في أنظمة التشغيل والتطبيقات.
1-6 يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أجهزة المستخدمين والأجهزة المحمولة.
1-7 يجب تزويد أجهزة المستخدمين والأجهزة المحمولة برسالة نصيّة (Banner) لإتاحة الاستخدام المصرّح به.
1-8 يجب السماح فقط بقائمة محددة من التطبيقات (Application Whitelisting) ومنع تسرّب البيانات (Data Leakage Prevention) واستخدام أنظمة مراقبة البيانات وغيرها.
1-9 يجب تشفير وسائط التخزين الخاصة بأجهزة المستخدمين والأجهزة المحمولة الهامة والحساسة والتي لها صلاحيات متقدمة وفقاً لمعيار التشفير المعتمد في جمعية البر الخيرية بطلعة التمياط .
1-10 يجب منع استخدام وسائط التخزين الخارجية، ويجب الحصول على إذن مسبق من إدارة تقنية المعلومات لامتلاك صلاحية استخدام وسائط التخزين الخارجية.
1-11 يجب عدم السماح لأجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) المزوّدة ببرمجيات غير محدثة أو منتهية الصلاحية (بما في ذلك أنظمة التشغيل والبرامج والتطبيقات) بالاتصال بشبكة جمعية البر الخيرية بطلعة التمياط لمنع التهديدات الأمنية الناشئة عن البرمجيات منتهية الصلاحية غير المحمية بحزم التحديثات والإصلاحات.
1-12 يجب أن تمُنَع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) غير المزوّدة بأحدث برمجيات الحماية من الاتصال بشبكة جمعية البر الخيرية بطلعة التمياط لتجنب حدوث المخاطر السيبرانية التي تؤدي إلى الوصول غير المصرّح به أو دخول البرمجيات الضارة أو تسرّب البيانات. وتتضمّن برمجيات الحماية برامج إلزامية، مثل: برامج الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware)، وجدار الحماية للمستضيف (Host-Based Firewall)، وأنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات في المستضيف (Host-based Intrusion Detection/Prevention)

1-13 يجب ضبط إعدادات أجهزة المستخدمين والأجهزة المحمولة غير المستخدمة بحيث تعرض شاشة توقّف محمية بكلمة مرور في حال عدم استخدام الجهاز (Session Timeout) لمدة <5 دقائق>.

1-14 يجب إدارة أجهزة المستخدمين والأجهزة المحمولة مركزياً من خلال خادم الدليل النشط (Active Directory) الخاص بنطاق جمعية البر الخيرية بطلعة التمياط أو نظام إداري مركزي.

1-15 يجب ضبط إعدادات أجهزة المستخدمين والأجهزة المحمولة بإدارة الوحدات التنظيمية المناسبة (Domain Controller) لتطبيق السياسات الملائمة وتثبيت الإعدادات البرمجية اللازمة.

1-16 يجب تنفيذ سياسات النطاق المناسبة (Group Policy) في جمعية البر الخيرية بطلعة التمياط وتطبيقها في جميع أجهزة المستخدمين والأجهزة المحمولة لضمان التزام جمعية البر الخيرية بطلعة التمياط بالضوابط التنظيمية والأمنية.

1 - متطلبات الأمن السيبراني لأمن أجهزة المستخدمين

2-1 يجب تخصيص أجهزة المستخدمين للفريق التقني ذي الصلاحيات الهامة، وأن تكون معزولة في شبكة خاصة لإدارة الأنظمة (Management Network) ولا ترتبط بأي شبكة أو خدمة أخرى.

2-2 يجب ضبط إعدادات أجهزة المستخدمين الهامة والحساسة والتي لها صلاحيات متقدمة لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني، مع عدم إمكانية إيقافه عن طريق المستخدم.

2-3 يجب تأمين أجهزة المستخدمين مادياً داخل مباني جمعية البر الخيرية بطلعة التمياط .

2- متطلبات الأمن السيبراني لأمن الأجهزة المحمولة

3-1 يجب منع وصول الأجهزة المحمولة إلى الأنظمة الحساسة إلا لفترة مؤقتة فقط، وذلك بعد إجراء تقييم المخاطر وأخذ الموافقات اللازمة من <الإدارة المعنية بالأمن السيبراني>.(CSCC-2-5-1-1))

3-2 يجب تشفير أقراص الأجهزة المحمولة التي تملك صلاحية الوصول للأنظمة الحساسة تشفيراً كاملاً (CSCC-2-5-1-2) .(Full Disk Encryption)

3 -متطلبات الأمن السيبراني لأمن الأجهزة الشخصية (BYOD)

4-1 يجب إدارة الأجهزة المحمولة مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management" MDM").

4-2 يجب فصل وتشفير البيانات والمعلومات الخاصة بـجمعية البر الخيرية بطلعة التمياط المخزنة على الأجهزة الشخصية للعاملين (BYOD).

4 - متطلبات أخرى

5-1 إجـراء نسـخ احتيـاطي دوري للبيـانات المخـزّنة على أجهـزة المستـخدميـن والأجهزة المحمولة، وذلك وفقاً لسياسة النسخ الاحتياطية المعتـمدة في جمعية البر الخيرية بطلعة التمياط .

5-2 تُحذَف بيـانـات جمعية البر الخيرية بطلـعة التميـاط المُخـزّنة عـلى الأجهـزة المحمولة والأجهزة الشخصية (BYOD) في الحالات التالية :

- فقدان الجهاز المحمول أو سرقته.
- انتـهاء أو إنهـاء العلاقة الوظيـفية بيـن المستـخدم وجمعيـة البر الخيـرية بطلعة التمياط .

5-3 يجب نشر الوعي الأمني للعاملين حول آلية استخدام الأجهزة ومسؤولياتهم تجـاهها وفقاً لسيـاسة الاستخدام المقبـول المعتـمدة في جمعية البر الخيرية بطلعة التمياط وإجراء جلسات توعية خاصة بالمستخدمين ذوي الصلاحيات الهامة والحساسة.

5-4 يجب استخدام مؤشر قيـاس الأداء (KPI) لضمـان التطويـر المستمر لحمـاية أجهزة المستخدمين والأجهزة المحمولة.

5-5 يجب مراجعة سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

1 - راعي ومالك وثيقة السياسة : مسؤول تقنية المعلومات.
2 - مراجعة السياسة وتحديثها : إدارة تقنية المعلومات.
3 - تنفيذ السياسة وتطبيقها : إدارة تقنية المعلومات.

الالتزام بالسياسة

1. يجب على مسؤول تقنية المعلومات ضمان التزام جمعية البر الخيرية بطلعة التمياط بهذه السياسة دورياً.
2. يجب على إدارة تقنية المعلومات وجميع الادارات في جمعية البر الخيرية بطلعة التمياط الالتزام بهذه السياسة.
3. قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية البر الخيرية بطلعة التمياط .