جمعية البر الأهلية بمركز بدائع العضيان

سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية

سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية

لجمعية البر الأهلية بمركز بدائع العضيان

مقدمة

تعد أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية من الأصول الحيوية في بيئة العمل الحديثة ومع ذلك، فإن استخدام هذه الأجهزة يمكن أن يزيد من مخاطر الأمن السيبراني، حيث يمكن أن تكون عرضة للهجمات والاختراقات لذلك، فإن وضع سياسة أمن لأجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية يعد أمرًا ضروريًا لحماية البيانات والأنظمة من المخاطر الأمنية، وفي ما يلي سياسة أمن لأجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية، والتدابير التي يمكن اتخاذها لضمان أمان هذه الأجهزة وحماية البيانات الحساسة.

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 (Bring Your Own Device" BYOD") داخل جمعية البر الأهلية بمركز بدائع العضيان، وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي سرية المعلومات وسلامتها وتوافرها.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية و أفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضوابط رقم ٢-٣-١ و٢-٦-١ 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 الأهلية بمركز بدائع العضيان " وتنطبق على جميع العاملين في جمعية البر الأهلية بمركز بدائع العضيان.

بنود السياسة

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.

2-1 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 الأهلية بمركز بدائع العضيان.

3-1 يجب تطبيق ضوابط الإعدادات والتحصين (Configuration and Hardening) لأجهزة المستخدمين والأجهزة المحمولة وفقاً لمعايير الأمن السيبراني.

4-1 يجب عدم منح العاملين صلاحيات هامة وحساسة (Privileged Access) على أجهزة المستخدمين والأجهزة المحمولة، ويجب منح الصلاحيات وفقاً لمبدأ الحد الأدنى من الصلاحيات والامتيازات.

5-1 يجب حذف أو إعادة تسمية حسابات المستخدم الافتراضية في أنظمة التشغيل والتطبيقات.

6-1 يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أجهزة المستخدمين والأجهزة المحمولة.

7-1 يجب تزويد أجهزة المستخدمين والأجهزة المحمولة برسالة نصيّة (Banner) لإتاحة الاستخدام المصرّح به.

8-1 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 الأهلية بمركز بدائع العضيان.

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 الأهلية بمركز بدائع العضيان لمنع التهديدات الأمنية الناشئة عن البرمجيات منتهية الصلاحية غير المحمية بحزم التحديثات والإصلاحات.

1-12 يجب أن تُمنَع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) غير المزوّدة بأحدث برمجيات الحماية من الاتصال بشبكة جمعية البر الأهلية بمركز بدائع العضيان 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)، و أنظمة 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 الأهلية بمركز بدائع العضيان 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 الأهلية بمركز بدائع العضيان وتطبيقها في جميع أجهزة المستخدمين والأجهزة المحمولة لضمان التزام جمعية البر الأهلية بمركز بدائع العضيان بالضوابط التنظيمية والأمنية.

متطلبات الأمن السيبراني لأمن أجهزة المستخدمين

1-2 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.

3-2 يجب تأمين أجهزة المستخدمين مادياً داخل مباني جمعية البر الأهلية بمركز بدائع العضيان.

متطلبات الأمن السيبراني لأمن الأجهزة المحمولة

1-3 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)

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

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 بجمعية البر الأهلية بمركز بدائع العضيان المخزنة على الأجهزة الشخصية للعاملين (BYOD).

متطلبات أخرى

5-1 إجراء نسخ احتياطي دوري للبيانات المخزّنة على أجهزة المستخدمين والأجهزة المحمولة، وذلك وفقاً لسياسة النسخ الاحتياطية المعتمدة في جمعية البر الأهلية بمركز بدائع العضيان.

5-2 تُحذَف بيانات جمعية البر الأهلية بمركز بدائع العضيان المُخزّنة على الأجهزة المحمولة والأجهزة الشخصية (BYOD) في الحالات التالية:

- فقدان الجهاز المحمول أو سرقته.
- انتهاء أو إنهاء العلاقة الوظيفية بين المستخدم وجمعية البر الأهلية بمركز بدائع العضيان.

5-3 يجب نشر الوعي الأمني للعاملين حول آلية استخدام الأجهزة ومسؤولياتهم تجاهها وفقاً لسياسة الاستخدام المقبول المعتمدة في جمعية البر الأهلية بمركز بدائع العضيان وإجراء جلسات توعية خاصة بالمستخدمين ذوي الصلاحيات الهامة والحساسة.

5-4 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية 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 الأهلية بمركز بدائع العضيان بهذه السياسة دورياً.
2. يجب على إدارة تقنية المعلومات وجميع الادارات في جمعية البر الأهلية بمركز بدائع العضيان الالتزام بهذه السياسة.
3. قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية البر الأهلية بمركز بدائع العضيان.

اعتماد مجلس الإدارة

الحمد لله والصلاة والسلام على رسول الله صلى لله عليه وسلم ... وبعد

فقد اطلع مجلس إدارة جمعية البر الخيرية بمركز بدائع العضيان في اجتماعه رقم (4) يوم الأحد بتاريخ: 2025/03/16م على سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (الإصدار الثاني 2025) وقرر اعتمادها والعمل بموجبها ونشرها على الموقع الإلكتروني للجمعية وفق الصيغة المرفقة بالاعتماد.

م	الاسم	الصفة	التوقيع
1	عبدالوهاب بن عبدالله العضياني	رئيس مجلس الإدارة	
2	مسلم بن برجس العضياني	نائب رئيس مجلس الإدارة	
3	عبدالرحمن بن عبدالعزيز العضياني	عضو مجلس الإدارة	
4	عبدالإله بن عبدالوهاب العضياني	عضو مجلس الإدارة	
5	صالح بن عبدالوهاب العضياني	عضو مجلس الإدارة	