سياسة أمن أجهزة المستخدمين

تم الاعتماد بمجلس إدارة جمعية التنمية الأسرية بمنطقة الباحة مَعين والمعتمد لدى المركز الوطني لتنمية القطاع الغير ربحي بخطاب تشكيل المجلس رقم NBM 015268 في تاريخ: ٢٠٢٣/١٢/١٤م والمعاد تشكيله بخطاب رقم EBM 018943 بتاريخ: ٢٠٢٤/٠٩/٢٤م حتى تاريخ:٢٠٢٧/١٢/١٤م

المملكة العربية السعودية
جمعية التنمية الأسرية بمنطقة الباحة (معين)
مسجلة بوزارة الموارد البشرية والتنمية الاجتماعية
برقم ٣٩٠
تحت اشراف مركز التنمية الاجتماعية بالباحة

تم التحديث والاعتماد بمحضر مجلس الإدارة رقم:٠٢ - ٢٠٢٤م بتاريخ: ٢٠٢٤/٠٦/١٢م، وبقرار اداري رقم:٢٠٢٤-٩٤ بتاريخ:٢٠٢٤/٠٦/٢٥م

باركود الاطلاع على الاعتمادات والتعديلات

مقدمة

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية الناتجة عن استخدام أجهزة المستخدمين (Workstations)، والأجهزة المحمولة (Devices Mobile)، والأجهزة الشخصية للعاملين (Bring Your Own Device "BYOD") داخل جمعية التنمية الأسرية بمنطقة الباحة (معين) 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-١:٢٠١٨) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لـــجمعية مَعين وتنطبق على جميع العاملين في جمعية التنمية الأسرية (معين)بمنطقة الباحة، وتعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعاييره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات جمعية مَعين الداخلية، مثل: عمليات الموارد البشـــرية، عمليات إدارة الموردين، عمليات إدارة المشاريع، إدارة التغيير وغيرها.

الأدوار والمسؤوليات

١- راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.

٢- مراجعة السياسة وتحديثها: إدارة تقنية المعلومات.

٣- تنفيذ السياسة وتطبيقها: إدارة تقنية المعلومات.

الالتزام بالسياسة

١. يجب على مسؤول تقنية المعلومات ضمان التزام جمعية التنمية الأسرية بمنطقة الباحة (معين) بهذه السياسة دورياً.

٢. يجب على إدارة تقنية المعلومات وجميع الادارات في جمعية التنمية الأسرية بمنطقة الباحة (معين) الالتزام بهذه السياسة.

٣. قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية التنمية الأسرية بمنطقة الباحة (معين).

بنود السياسة

١ البنود العامة

١-١ 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.

١-٢ 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 التنمية الأسرية بمنطقة الباحة (معين).

١-٣ يجب تطبيق ضوابط الإعدادات والتحصين (Configuration and Hardening) لأجهزة المستخدمين والأجهزة المحمولة وفقاً لمعايير الأمن السيبراني.

١-٤ يجب عدم منح العاملين صلاحيات هامة وحساسة (Privileged Access) على أجهزة المستخدمين والأجهزة المحمولة، ويجب منح الصلاحيات وفقاً لمبدأ الحد الأدنى من الصلاحيات والامتيازات.

١-٥ يجب حذف أو إعادة تسمية حسابات المستخدم الافتراضية في أنظمة التشغيل والتطبيقات.

١-٦ يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أجهزة المستخدمين والأجهزة المحمولة.

١-٧ يجب تزويد أجهزة المستخدمين والأجهزة المحمولة برسالة نصيّة (Banner) لإتاحة الاستخدام المصرّح به.

١-٨ يجب السماح فقط بقائمة محددة من التطبيقات (Application Whitelisting) ومنع تسرّب البيانات (Data Leakage Prevention) واستخدام أنظمة مراقبة البيانات وغيرها.

١-٩ يجب تشفير وسائط التخزين الخاصة بأجهزة المستخدمين والأجهزة المحمولة الهامة والحساسة والتي لها صلاحيات متقدمة وفقاً لمعيار التشفير المعتمد في جمعية التنمية الأسرية بمنطقة الباحة (معين).

١-١٠ يجب منع استخدام وسائط التخزين الخارجية، ويجب الحصول على إذن مسبق من إدارة تقنية المعلومات لامتلاك صلاحية استخدام وسائط التخزين الخارجية.

١-١١ 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 التنمية الأسرية بمنطقة الباحة (معين) لمنع التهديدات الأمنية الناشئة عن البرمجيات منتهية الصلاحية غير المحمية بحزم التحديثات والإصلاحات.

١-١٢ يجب أن تُمنَع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) غير المزوّدة بأحدث برمجيات الحماية من الاتصال بشبكة جمعية التنمية الأسرية بمنطقة الباحة (معين) 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

١-١٣ يجب ضبط إعدادات أجهزة المستخدمين والأجهزة المحمولة غير المستخدمة بحيث تعرض شاشة توقّف محمية بكلمة مرور في حال عدم استخدام الجهاز (Session Timeout) لمدة <٥ دقائق>.

١-١٤ يجب إدارة أجهزة المستخدمين والأجهزة المحمولة مركزياً من خلال خادم الدليل النشط (Active Directory) الخاص بنطاق جمعية التنمية الأسرية بمنطقة الباحة (معين) أو نظام إداري مركزي.

١-١٥ يجب ضبط إعدادات أجهزة المستخدمين والأجهزة المحمولة بإدارة الوحدات التنظيمية المناسبة (Domain Controller) لتطبيق السياسات الملائمة وتثبيت الإعدادات البرمجية اللازمة.

١-١٦ يجب تنفيذ سياسات النطاق المناسبة (Group Policy) في جمعية التنمية الأسرية بمنطقة الباحة (معين) وتطبيقها في جميع أجهزة المستخدمين والأجهزة المحمولة لضمان التزام جمعية التنمية الأسرية بمنطقة الباحة (معين) بالضوابط التنظيمية والأمنية.

٢ متطلبات الأمن السيبراني لأمن أجهزة المستخدمين

٢-١ 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.

٢-٢ 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.

٢-٣ يجب تأمين أجهزة المستخدمين مادياً داخل مباني جمعية التنمية الأسرية بمنطقة الباحة (معين).

٣ متطلبات الأمن السيبراني لأمن الأجهزة المحمولة

٣-١ 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-٢-٥-١-١)

٣-٢ يجب تشفير أقراص الأجهزة المحمولة التي تملك صلاحية الوصول للأنظمة الحساسة تشفيراً كاملاً (Full Disk Encryption). (CSCC-٢-٥-١-٢)

٤ متطلبات الأمن السيبراني لأمن الأجهزة الشخصية (BYOD)

٤-١ يجب إدارة الأجهزة المحمولة مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Device Management" MDM" Mobile).

٤-٢ يجب فصل وتشفير البيانات والمعلومات الخاصة بجمعية التنمية الأسرية بمنطقة الباحة (معين) المخزنة على الأجهزة الشخصية للعاملين (BYOD).

٥ متطلبات أخرى

٥-١ إجراء نسخ احتياطي دوري للبيانات المخزّنة على أجهزة المستخدمين والأجهزة المحمولة، وذلك وفقاً لسياسة النسخ الاحتياطية المعتمدة في جمعية التنمية الأسرية بمنطقة الباحة (معين).

٥-٢ تُحذَف بيانات جمعية التنمية الأسرية بمنطقة الباحة (معين) المُخزّنة على الأجهزة المحمولة والأجهزة الشخصية (BYOD) في الحالات التالية:

- فقدان الجهاز المحمول أو سرقته.
- انتهاء أو إنهاء العلاقة الوظيفية بين المستخدم وجمعية التنمية الأسرية بمنطقة الباحة (معين).

٥-٣ يجب نشر الوعي الأمني للعاملين حول آلية استخدام الأجهزة ومسؤولياتهم تجاهها وفقاً لسياسة الاستخدام المقبول المعتمدة في جمعية التنمية الأسرية بمنطقة الباحة (معين) وإجراء جلسات توعية خاصة بالمستخدمين ذوي الصلاحيات الهامة والحساسة.

٥-٤ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية أجهزة المستخدمين والأجهزة المحمولة.

٥-٥ يجب مراجعة سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية سنوياً، وتوثيق التغييرات واعتمادها.