٧-سياسة أمن أجهزة المستخدمين المحمولة.

المسؤول عنها	الاتصال المؤسسي
رمز السياسة	إعلام.س.٧
الحالة	معتمدة

-الاعتماد

الحمدالله والصلاة والسلام على رسول الله وبعد:

فقد اطلع أعضاء الجمعية العمومية بجمعية مكافحة السرطان الخيرية بالأحساء (تفاؤل) في اجتماعهم العادي يوم الإثنين الموافق ٢٠٢٢/٩/١٩م على **سياسة أمن أجهزة المستخدمين المحمولة.** وقرروا اعتمادها والعمل بموجبها ونشرها على الموقع الإلكتروني للجمعية وفق الصيغة المرفقة بالاعتماد.

رئيس مجلس الإدارة

محمد بن عبد العزيز العفالق

سياسة أمن أجهزة المستخدمين المحمولة.

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 مكافحة السرطان (تفاؤل)، وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي سرية المعلومات وسالمتها وتوافرها.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العالقة، وهي متطلب تشريعي كما هو مذكور في الضوابط رقم ٢-٣-١ و٢-٦-١ من الضوابط الأساسية لألمن 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 مكافحة السرطان (تفاؤل) وتنطبق على جميع العاملين في جمعية مكافحة السرطان (تفاؤل).

بنود السياسة:

١ -البنود العامة

١-١ يجب حماية البيانات والمعلومات المخزنة في أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD)حسب تصنيفها باستخدام الضوابط الأمنية المناسبة لتقييد الوصول إلى هذه المعلومات، ومنع العاملين غير المصرح 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 مكافحة السرطان (تفاؤل).

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

١-٤ يجب عدم منح العاملين صلاحيات هامة وحساسة (Privileged Access)على أجهزة المستخدمين والأجهزة المحمولة ويجب منح الصلاحيات وفقا 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 المصرح به.

١-٨ يجب السماح فقط بقائمة محددة من التطبيقات (Whitelisting Application) ومنع تسرب 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 وفقا لمعيار التشفير المعتمد في جمعية مكافحة السرطان (تفاؤل).

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

١-١١ يجب عدم السماح لأجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD)المزّودة ببرمجيات غير محدثة أو منتهية الصالحية (بما في ذلك

أنظمة التشغيل والبرامج والتطبيقات) بالاتصال بشبكة جمعية مكافحة السرطان (تفاؤل) 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 المزّودة بأحدث برمجيات الحماية من الاتصال بشبكة جمعية مكافحة السرطان (تفاؤل) لتجنب حدوث المخاطر السيبرانية التي تؤدي إلى الوصول غير المصرح به أو دخول البرمجيات الضارة أو تسرب البيانات. وتتضمن برمجيات الحماية برامج إلزامية، مثل: برامج الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) وجدار الحماية للمستضيف (Based Firewall-Host) 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 توقف 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 مكافحة السرطان (تفاؤل) أو نظام إداري مركزي.

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

١-١ يجب تنفيذ سياسات النطاق المناسبة (Group Policy) في جمعية مكافحة السرطان (تفاؤل) وتطبيقها في جميع أجهزة المستخدمين والأجهزة المحمولة لضمان التزام جمعية مكافحة السرطان (تفاؤل) بالضوابط التنظيمية والأمنية.

٢ -متطلبات الأمن السيبراني الأمن 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 مكافحة السرطان (تفاؤل).

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 إدارة تقنية المعلومات. (CSCC-٢-٥-١-١)

٣-٢ يجب تشفير أقراص الأجهزة المحمولة التي تملك صلاحية الوصول للأنظمة الحساسة تشفيراً كاملًا

(CSCC-2-5-1-2).(Full Disk Encryption)

٤ -متطلبات الأمن السيبراني لأمن الأجهزة الشخصية(BYOD)

٤-١ يجب إدارة الأجهزة المحمولة مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device

(" Management" MDM.

٤-٢ يجب فصل وتشفير البيانات والمعلومات الخاصة بـجمعية مكافحة السرطان (تفاؤل) المخزنة على الأجهزة الشخصية للعاملين (BYOD).

٥ -متطلبات أخرى:

٥-١ إجراء نسخ احتياطي دوري للبيانات المخزنة على أجهزة المستخدمين والأجهزة المحمولة، وذلك لسياسة النسخ الاحتياطية المعتمدة في جمعية مكافحة السرطان (تفاؤل) .

٥-٢ تُحذف بيانات جمعية مكافحة السرطان (تفاؤل) المخزنة على الأجهزة المحمولة والأجهزة الشخصية (BYOD) في الحالات التالية:

• فقدان الجهاز المحمول أو سرقته.

• انتهاء أو إنهاء العلاقة الوظيفية بين المستخدم وجمعية مكافحة السرطان (تفاؤل)

٥-٣ يجب نشر الوعي الأمني للعاملين حول آلية استخدام الأجهزة ومسؤولياتهم تجاهها وفقاً لسياسة الاستخدام المقبول المعتمدة في جمعية مكافحة السرطان (تفاؤل) وإجراء جلسات توعية خاصة بالمستخدمين ذوي الصالحيات 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.

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 مكافحة السرطان (تفاؤل) بهذه السياسة دورياً.

٢ -يجب على الإدارة المعنية بتقنية المعلومات وجميع الإدارات في جمعية مكافحة السرطان (تفاؤل) الالتزام بهذه السياسة.

٢ -قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية مكافحة السرطان (تفاؤل).