هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج سياسة الحماية من البرمجيات الضارة

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة.
وللقيام بذلك، اتبع الخطوات التالية:

- اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
- أضف "<اسم الجهة>" في مربع البحث عن النص.
- أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
- اضغط على "المزيد" وتأكّد من اختيار "Match case".
- اضغط على "استبدل الكل".
- أغلق مربع الحوار.

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدِّلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف التعديل>

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

اختر التصنيف

الإصدار <١,٠>

قائمة المحتويات

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة حماية الأصول المعلوماتية والتقنية من البرمجيات الضارة في <اسم الجهة> لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية وذلك لتحقيق الأهداف الرئيسية للحماية وهي: سرية المعلومات، وسلامة أنظمة المعلومات، وتوافرها.

تمت موائمة هذه السياسة مع الضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

تطبق هذه السياسة على جميع الأصول المعلوماتية والتقنية (مثل أجهزة المستخدمين، الأجهزة المحمولة والخوادم) الخاصة ب<اسم الجهة>، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب على <اسم الجهة> توفير تقنيات وآليات الحماية المناسبة والحديثة والمتطورة والعصرية والموثوقة.

١-٢ يجب تطبيق التقنيات والآليات المناسبة لحماية جميع أجهزة المستخدمين والأجهزة المحمولة والخوادم والأنظمة والتطبيقات من البرمجيات الضارة (Malware) وإدارتها بشكل آمن.

١-٣ يجب التأكد من أن تقنيات وآليات الحماية قادرة على اكتشاف جميع أنواع البرمجيات الضارة، (مثل الفيروسات (Virus)، وأحصنة طروادة (Trojan Horse)، والديدان (Worms)، وبرمجيات التجسس (Spyware)، وبرمجيات الإعلانات المتسللة (Adware)، ومجموعة الجذر (Root Kits) وغيرها من البرمجيات الضارة).

١-٤ يجب التأكد من ملائمة تقنيات وآليات الحماية لأنظمة التشغيل مثل أنظمة ويندوز (Windows)، وأنظمة يونكس (UNIX)، وأنظمة لينكس (Linux)، ونظام ماك (Mac)، وغيرها من الأنظمة الخاصة ب<اسم الجهة> وكذلك توافقها للتكامل الآمن مع أنظمة المعلومات الخاصة ب<اسم الجهة> قبل اختيارها.

١-٥ يجب اختبار تحديثات أنظمة الحماية في بيئة غير بيئة التشغيل والإنتاج الفعلية للتأكد من سلامتها قبل تطبيقها على البيئة التشغيلية.

١-٦ يجب التأكد من أن تقنيات الحماية قادرة على استعادة التعريفات إلى النسخ السابقة في حال تسبب تحديثها بضرر للأنظمة أو متطلبات الأعمال.

١-٧ يجب تطبيق آليات الوصول والصلاحيات الخاصة بإدارة وتشغيل تقنيات الحماية والأنشطة الخاصة بها من تعطيل أو تغيير ونحوها وتقييدها لمشرفي أنظمة الحماية ومراجعتها بشكل دوري وذلك وفق السياسات المعتمدة ذات العلاقة لدى <اسم الجهة>.

١-٨ يجب تقييد صلاحيات تعطيل التثبيت أو إلغائه أو تغيير إعدادات تقنيات الحماية من البرمجيات الضارة ومنحها لمشرفي نظام الحماية فقط.

١-٩ يجب على <الإدارة المعنية بالأمن السيبراني> التأكد من الوعي الأمني اللازم لدى جميع العاملين للتعامل مع البرمجيات الضارة والتقليل من مخاطرها.

١-١٠ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات الحماية لأجهزة المستخدمين والخوادم أو الأطراف الخارجية من البرمجيات الضارة.

٢- إعدادات تقنيات وآليات الحماية من البرمجيات الضارة

٢-١ يجب ضبط إعدادات تقنيات الحماية وآلياتها وفقًا للمعايير التقنية الأمنية المعتمدة لدى <اسم الجهة>، مع الأخذ بالاعتبار إرشادات المورد وتوصياته.

٢-٢ يجب ضبط إعدادات برامج مكافحة الفيروسات على خوادم البريد الإلكتروني لفحص جميع رسائل البريد الإلكتروني الواردة والصادرة.

٢-٣ يجب ضبط إعدادات برامج مكافحة الفيروسات على خوادم البريد الإلكتروني لتقييد استقبال أو إرسال مرفقات البريد الإلكتروني وفقًا لنوع الملف، ولمحتوى الملف.

٢-٤ يجب تحديث برامج مكافحة الفيروسات دوريًا وفقًا لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة لدى <اسم الجهة>.

٢-٥ يجب أن يكون التحديث أحد متطلبات عمل الأجهزة الطرفية.

٢-٦ يجب ضمان توافر خوادم برامج الحماية من البرمجيات الضارة، كما يجب أن تكون برامج الحماية من البرمجيات الضارة متوافقة مع البيئة الاحتياطية المخصصة للمهام والأعمال غير الحساسة.

٢-٧ يجب تصفية رسائل البريد الإلكتروني (Filtering) وذلك باستخدام تقنيات الحماية الحديثة.

٢-٨ يجب منع الوصول إلى المواقع الإلكترونية والمصادر الأخرى على الإنترنت المعروفة باستضافتها لبرمجيات ضارة وذلك باستخدام آلية تصفية محتوى الويب (Filtering Web Content).

٢-٩ يجب مزامنة التوقيت (Clock Synchronization) مركزيًا ومن مصدر دقيق وموثوق لجميع تقنيات وآليات الحماية من البرمجيات الضارة.

٢-١٠ يجب ضبط إعدادات تقنيات الحماية من البرمجيات الضارة للقيام بعمليات التحقق من المحتوى المشبوه في مصادر معزولة مثل صندوق الفحص (Sandbox).

٢-١١ يجب القيام بعمليات مسح دورية لأجهزة المستخدمين والخوادم والتأكد من سلامتها من البرمجيات الضارة.

٢-١٢ يجب إجراء عمليات المسح لوسائط التخزين في بيئة مخصصة لهذا الغرض قبل استخدامها من خارج <اسم الجهة> أو استخدام وسائط التخزين الخاصة ب<اسم الجهة> على أنظمة لا تتبع ل<اسم الجهة> أو باستخدام خدمة فحص الملفات والروابط، ضمن البوابة الوطنية لخدمات الأمن السيبراني "حصين".

٢-١٣ يجب تقييد استخدام وسائط التخزين الخارجية في بيئة الإنتاج، مالم يتم تطوير آليات آمنة وتطبيقها لنقل البيانات لبيئة الانتاج.

٢-١٤ يجب تقييد استخدام تقنيات وسائط التخزين القابلة للإزالة وأخذ الموافقات اللازمة للاستخدام.

٢-١٥ يجب التقييد والتقسيم والفصل المادي والمنطقي عند ربط أنظمة أو أجهزة <اسم الجهة> مع شبكات خارجية، مثل: الإنترنت أو الدخول عن بعد أو الاتصال اللاسلكي.

٢-١٦ يجب تحديث تقنيات الحماية من البرمجيات الضارة تلقائيًا عند توفر إصدارات جديدة من المورد، مع الأخذ بالاعتبار سياسة إدارة التحديثات والإصلاحات.

٢-١٧ يجب توفير تقنيات حماية البريد الإلكتروني وتصفح الإنترنت من التهديدات المتقدمة المستمرة (APT Protection)، والتي تستخدم عادةً الفيروسات والبرمجيات الضارة غير المعروفة مسبقًا (Zero-Day Malware)، وتطبيقها وإداراتها بشكل آمن.

٢-١٨ يجب توفير تقنيات لاكتشاف الأوامر المنفذة (Command Execution) وفحصها.

٢-١٩ يجب توفير تقنيات لاكتشاف وفحص جلسات الاتصالات الحديثة (New Communication Sessions).

٢-٢٠ يجب ضبط إعدادات تقنيات الحماية بالسماح لقائمة محددة فقط (Whitelisting) من ملفات التشغيل للتطبيقات والبرامج للعمل على الخوادم وجميع الأجهزة (بما فيها الخوادم والنهايات الطرفية) الخاصة بجميع الأنظمة.

٢-٢١ يجب حماية جميع أجهزة المستخدمين والخوادم عن طريق تقنيات حماية الأجهزة الطرفية (End-point Protection) المعتمدة لدى <اسم الجهة>.

٢-٢٢ 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 <رئيس الإدارة المعنية بالأمن السيبراني>.

٢-٢٣ يجب إدارة تقنيات الحماية من البرمجيات الضارة مركزيًا ومراقبتها باستمرار.

الأدوار والمسؤوليات

١- **مالك السياسة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

٢- **مراجعة السياسة وتحديثها:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بتقنية المعلومات> و<الإدارة المعنية بالأمن السيبراني>.

٤- **قياس الالتزام بالسياسة:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة السياسة سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالسياسة

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> في <اسم الجهة> التأكد من التزام <اسم الجهة> بهذه السياسة دوريًا.

٢- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذه السياسة.

٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.