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 معيار 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.

اختر التصنيف

الإصدار <١,٠>

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

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذا المعيار هو المساعدة على تطبيق متطلبات الأمن السيبراني وسياسة الحماية من البرمجيات الضارة في <اسم الجهة> وذلك لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية بغرض تحقيق الأهداف الرئيسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تتوافق المتطلبات الواردة في هذا المعيار مع سياسة الحماية من البرامج الضارة ومتطلبات الأمن السيبراني وتمت موائمة هذا المعيار مع الضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

يغطي هذا المعيار جميع الأصول المعلوماتية والتقنية (مثل أجهزة المستخدمين، الأجهزة المحمولة والخوادم) الخاصة ب<اسم الجهة> وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

١	تطبيق تقنيات وآليات الحماية من البرمجيات الضارة (Malware Protection (Solution Implementation
الهدف	ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية ل<اسم الجهة>، وذلك بتطبيق تقنيات وآليات للحماية من البرمجيات الضارة.
المخاطر المحتملة	يُعد غياب تقنيات وآليات الحماية من البرمجيات الضارة سببًا أساسيًا في انتهاك سرية أو سلامة أو توافر البيانات أو التطبيقات أو نظم التشغيل نتيجة تسرب البرمجيات الضارة بمختلف أنواعها إلى أجهزة معالجة المعلومات الخاصة ب<اسم الجهة>.
الإجراءات المطلوبة	
١-١	أن تتمتع تقنيات وآليات الحماية من البرمجيات الضارة بالقدرات التالية: • منع البرمجيات الضارة. • اكتشاف البرمجيات الضارة.
١-٢	أن تتمتع تقنيات وآليات الحماية من البرمجيات الضارة بالقدرات اللازمة للحماية من مختلف أنواع البرمجيات الضارة على سبيل المثال لا الحصر: • الفيروسات. • الديدان الحاسوبية.

	• فيروسات حصان طروادة. • برامج التجسس. • البرمجيات الضارة غير المعروفة مسبقًا. • برامج الفدية. • برامج تسجيل المفاتيح.
١-٣	ضبط إعداد تقنيات وآليات الحماية من البرمجيات الضارة لحماية الأجهزة والأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة> بما في ذلك: • جدار الحماية. • خوادم البريد الإلكتروني. • خوادم شبكة الويب. • الخوادم الوكيلة. • خوادم الوصول عن بُعد. • أجهزة المستخدمين. • الأجهزة المحمولة. • نظام أسماء النطاقات. • بروتوكول التهيئة الآلية للمضيفين.
١-٤	أن تتمتع كل تقنية وآلية الحماية من البرمجيات الضارة بلوحة تحكم مركزية، مما يضمن التطبيق المتسق لسياسة الحماية من البرمجيات الضارة على جميع الأجهزة ومراقبة تهديدات هذه البرمجيات الضارة.
١-٥	أن تتكامل تقنيات وآليات الحماية من البرمجيات الضارة لتؤدي الوظائف التالية: • برامج مكافحة الفيروسات. • نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات. • جدار الحماية. • تصفية/فحص المحتوى. • السماح بقائمة محددة من التطبيقات. • صندوق الفحص. • اكتشاف نقطة النهاية والاستجابة. • نظام منع التطفل القائم على المضيف والشبكات. • نظام كشف التسلل المستند إلى المضيف. وأن تُحدد وظائف تقنيات وآليات الحماية من البرمجيات الضارة بناءً على مخرجات عملية تقييم المخاطر.
١-٦	إرسال سجلات الأحداث المتعلقة باكتشاف ومنع البرمجيات الضارة إلى تقنية الحماية من البرمجيات الضارة وإلى نظام سجلات الأحداث ومراقبة الأمن السيبراني لمراقبة

	الأحداث وتحليلها، وتحديد أوجه الارتباط، واتخاذ القرار مع ضرورة الأتمتة قدر الإمكان.
١-٧	الاستمرار على تطبيق آليات الحماية من البرمجيات الضارة للحد من أثر تهديدات البرمجيات الضارة في حال حدوثها. وتشمل هذه الآليات ما يلي: • الحماية عبر إعدادات نظام الإدخال/الإخراج الأساسي (BIOS). • آلية فصل التطبيقات غير الموثوقة باستخدام صندوق الفحص. • الفصل بين استخدامات المتصفح للتطبيقات الرسمية للجهة والغير الرسمية. • الفصل من خلال الأنظمة الافتراضية. • تقييد التفعيل التلقائي للملفات التي يتم تنزيلها أو البرامج المشتركة أو البرامج المجانية. • اقتصار صلاحيات المستخدم النهائي على الجهاز الذي يستخدمه (دون منحه حقوق إدارية). • تقييد التفعيل التلقائي أو استخدام الملفات المحتوية على حزم (Macros). • حجب أنظمة التحميل والتشغيل (Booting Systems) الموجودة على الأقراص المرنة أو الأقراص المدمجة، إلا في الحالات الطارئة أو عند استخدام وسائط موثوقة. • إعداد كافة البرمجيات لتنبيه المستخدم في حال فتح ملفات تحتوي على حزم (Macros). • تعطيل الاتصال المباشر من جهاز إلى جهاز.
١-٨	أن يكون إجراء إزالة تثبيت برنامج تقنيات وآليات الحماية من البرمجيات الضارة محميًا بكلمة مرور وتتم إدارته ومراقبته عن بعد لضمان عدم قدرة المستخدم على إزالة تثبيت البرنامج أو تغيير إعداداته أو إلغاء تفعيله وتفعيل سجلات الأحداث لهذا النشاط.
٢	إعدادات تقنيات وآليات الحماية من البرمجيات الضارة (Malware Protection (Solution Configuration
الهدف	التأكد من تطبيق الإعدادات الصحيحة لتقنيات وآليات الحماية من البرمجيات الضارة وذلك لتوفير الحماية الفعالة من تهديدات البرمجيات الضارة.
المخاطر المحتملة	تؤدي الإعدادات غير المكتملة لتقنيات وآليات الحماية من البرمجيات الضارة إلى انتشار البرمجيات الضارة غير المكتشفة في بيئة <اسم الجهة> وبالتالي تقليل فعالية الحل بشكل عام.

المعايير المطلوبة	
٢-١	ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة لإجراء فحص مباشر لجميع الملفات عند الوصول إليها أو نسخها أو نقلها وتنفيذها لضمان اكتشاف جميع البرمجيات الضارة قبل تنشيطها.
٢-٢	ضبط إعداد برنامج تقنيات وآليات الحماية من البرمجيات الضارة لإجراء فحص كامل للنظام أسبوعيًا على الأقل، ويمكن أن يكون وقت الفحص عند تشغيل النظام أو خلال ساعات الاستخدام المنخفض.
٢-٣	تمكين خاصية فحص مكافحة البرمجيات الضارة للوسائط القابلة للإزالة تلقائيًا عند إدخالها أو توصيلها.
٢-٤	ضبط وإعداد الأجهزة على مستوى المستخدم بصورة تمنع التشغيل التلقائي للمحتوى أو التحميل.
٢-٥	تفعيل خاصية التنبيه وتسجيل استعلامات نظام أسماء النطاقات (DNS) للكشف عن الاستعلامات الخاصة بنطاقات نظام أسماء النطاقات (DNS) الضارة المعروفة.
٢-٦	تفعيل ميزات مكافحة الاستغلال وتنبيه وتسجيل الأحداث على نظام التشغيل لاكتشاف و/أو منع الأنشطة المشبوهة والضارة.
٢-٧	ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة لاكتشاف البرمجيات الضارة أولًا ثم الاستجابة لها في بيئة مخصصة على النحو التالي: تطهير البرمجيات الضارة، أو حذفها، أو عزلها أو تشفيرها.
٢-٨	ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة بحيث يقوم بعزل الملفات التي أصابها الفيروس في حال عدم القدرة على حذفها.
٢-٩	ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة بحيث يقوم بتنبيه المستخدم بعدم قدرته على تنظيف أو عزل الشفرة الخبيثة.
٢-١٠	تثبيت تقنيات وآليات الحماية من البرمجيات الضارة على خوادم البريد الإلكتروني، بما في ذلك بوابة بروتوكول إرسال البريد البسيط (SMTP). يجب إعداد تقنيات وآليات الحماية من البرمجيات الضارة بحيث تقوم بمسح محتوى الرسائل والمرفقات في كافة رسائل البريد الإلكتروني. وفي حال العثور على برمجيات ضارة في بروتوكول إرسال البريد البسيط (SMTP) الوارد، يجب اتباع الإجراءات التالية: • حذف الفيروسات بالمرفقات المصابة. • عزل المرفقات المصابة في حال عدم القدرة على مسحها. • اتباع إجراءات إدارة الحوادث والاستجابة.

اختر التصنيف

الإصدار <١,٠>

٢-١١	ضبط إعدادات نظام التشغيل والتطبيقات على لوحة التحكم المركزية بتقنيات وآليات الحماية من البرمجيات الضارة مع مراعاة موائمة إعدادات المورد مع احتياجات الأعمال.
٢-١٢	منع الوصول إلى المواقع الإلكترونية والمصادر الأخرى على الإنترنت والمعروفة باستضافتها لمحتوى خبيث باستخدام آلية تصفية محتوى الويب.
٢-١٣	تقوم <اسم الجهة> بمراقبة الأداء فيما يتعلق بما يلي: • استخدام وحدة التحكم المركزية (CPU). • استخدام الذاكرة. • أداء الشبكة. • استخدام القرص.
٢-١٤	أن يقدم مشرفو تقنيات وآليات الحماية من البرمجيات الضارة تقاريرًا شهرية حول حالة الحماية من البرمجيات الضارة إلى <الإدارة المعنية بالأمن السيبراني> في <اسم الجهة>. ويجب أن يتضمن التقرير على الأقل ما يلي: • عدد أجهزة الحاسوب والخوادم وأجهزة الحاسوب المحمولة والأنظمة غير المحدثة بأحدث أنماط التواقيع. • أكثر ١٠ برمجيات ضارة تم اكتشافها. • عدد الفيروسات/الديدان الحاسوبية/البرامج الخبيثة المكتشفة. • عدد الفيروسات/الديدان الحاسوبية/البرامج الخبيثة التي تم تنظيفها/عزلها/حذفها. • الإجراء المُتخذ لحل مشكلة الإصابة بالبرمجيات الضارة. • مصدر الإصابة.
٣	تحديثات تقنيات وآليات الحماية من البرمجيات الضارة (Malware Protection (Solution Updates
الهدف	ضمان تحديث تقنيات وآليات الحماية من البرمجيات الضارة لحماية الأصول المعلوماتية والتقنية من أحدث البرمجيات الضارة المعروفة.
المخاطر المحتملة	يمكن أن تمر أحدث البرمجيات الضارة المعروفة دون أن يتم كشفها، وقد تؤدي إلى انتهاك الأمن السيبراني لـ<اسم الجهة> في حال عدم تحديث تقنيات وآليات الحماية من البرمجيات الضارة بأحدث التواقيع.
المعايير المطلوبة	
٣-١	تحديث تقنيات وآليات الحماية من البرمجيات الضارة بشكل مستمر وتلقائي وفقًا لسياسة إدارة حزم التحديثات والإصلاحات.

٣-٢	التحقق من سلامة المعلومات والملفات الخاصة بتقنيات وآليات الحماية من البرمجيات الضارة دوريًا.
٣-٣	تحديث قاعدة بيانات تواقيع تقنيات وآليات الحماية من البرمجيات الضارة تلقائيًا أو يدويًا بشكل منتظم.
٣-٤	إعداد تقنيات وآليات الحماية من البرمجيات الضارة للحصول على نمط التواقيع من الموقع الإلكتروني المعتمد للمورد.
٣-٥	إعداد تقنيات وآليات الحماية من البرمجيات الضارة "لتوزيع" آخر تحديثات التواقيع على أجهزة المستخدمين والخوادم مع تنبيه مدير النظام في حال فشل تحديث التواقيع.
٣-٦	ضبط إعدادات الأجهزة غير الموجودة ضمن شبكة الأجهزة المحمولة في <اسم الجهة> لتتضمن خيارات تحديث بديلة بحيث يمكن تحديث التواقيع مباشرة من الموقع الإلكتروني المعتمد للمورد.
٣-٧	أن تدعم تقنيات وآليات الحماية من البرمجيات الضارة استرجاع تحديثات التواقيع في حال أدت آخر التحديثات إلى عدم اتساق برنامج مكافحة الفيروسات وأثرت على قدرته على العمل بالصورة المتوقعة.
٤	**تتبع التهديدات والثغرات الجديدة (Tracking New Threats and Vulnerabilities)**
الهدف	التحديد المبكر للتهديدات الجديدة التي يمكن أن تؤثر على أمن <اسم الجهة> وضمان اتخاذ الإجراءات المناسبة للحد من المخاطر المرافقة.
المخاطر المحتملة	يمكن أن تتعرض <اسم الجهة> لانتهاك أمني نتيجة عدم القدرة على كشف البرمجيات الضارة الخبيثة الجديدة وغير المعروفة.
المعايير المطلوبة	
٤-١	أن تتابع <اسم الجهة> التهديدات الجديدة الناشئة عن الشفرات الخبيثة ويجب أن تحتفظ بقائمة بكافة السيناريوهات المحتملة للإصابة بالبرمجيات الخبيثة (مثل: كيف يمكن للفيروس أن يؤثر على الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة> وما هي طريقة وصوله إليها).
٤-٢	ضبط تقنيات الحماية من البرمجيات الضارة للتعرف والاستجابة للبرمجيات الضارة اعتمادًا على حالات محددة وواضحة مسبقًا.
٤-٣	عند وجود ثغرات جديدة، يجب أن تحدد <اسم الجهة> الخطوات التي يجب اتخاذها لضمان الحد من المخاطر المحتملة.

٤-٤	مراقبة أداء البرامج والتطبيقات الأكثر استخدامًا لدى <اسم الجهة>، لرصد العمليات المشبوهة قبل انتشارها.

الأدوار والمسؤوليات

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

٢- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات> و<الإدارة المعنية بالأمن السيبراني>.

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

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا على الأقل أو عند حدوث تغييرات تقنية جوهرية في البنية التحتية أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالمعيار

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دوريًا.

٢- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا المعيار.

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