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

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

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

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل الاسم الكامل للشخص>	اضغط هنا لإضافة نص	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدّل بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

قائمة المحتويات

الأهداف 3
نطاق العمل وقابلية التطبيق 3
المعايير 3
الأدوار والمسؤوليات 13
الالتزام بالمعيار 13

الأهداف

الغرض من هذا المعيار هو تطبيق متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالحماية من البرمجيات الضارة في <اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية، وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٣-١-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> وينطبق هذا المعيار على جميع العاملين في <اسم الجهة>.

المعايير

1	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 لـ<اسم الجهة>، وذلك بتطبيق تقنيات وآليات للحماية من البرمجيات الضارة.
المخاطر المحتملة	يُعد غياب تقنيات وآليات الحماية من البرمجيات الضارة سبباً أساسياً في انتهاك سرية أو سلامة أو توافر البيانات أو التطبيقات أو نظم التشغيل نتيجة تسرب البرمجيات الضارة بمختلف أنواعها إلى أجهزة معالجة المعلومات الخاصة بـ<اسم الجهة>.
الإجراءات المطلوبة	
1-1	يجب أن تتمتع تقنيات وآليات الحماية من البرمجيات الضارة بالقدرات التالية: • منع البرمجيات الضارة • اكتشاف البرمجيات الضارة Malware protection solutions shall have the following capabilities: • Malware Prevention • Malware Detection

2-1	يجب أن تتمتع تقنيات وآليات الحماية من البرمجيات الضارة بالقدرات اللازمة للحماية من مختلف أنواع البرمجيات الضارة ومنها: • الفيروسات • الديدان الحاسوبية • فيروسات حصان طروادة • برامج التجسس • البرمجيات الضارة غير المعروفة مسبقًا Malware protection solutions shall have the capabilities to protect against different varieties of malware including but not limited to: • Viruses • Worms • Trojan Horses • Spyware • Zero-day malware
3-1	يجب إعداد تقنيات وآليات الحماية من البرمجيات الضارة لحماية النهايات الطرفية في الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> بما في ذلك: • جدار الحماية • خوادم البريد الإلكتروني • خوادم شبكة الويب • الخوادم الوكيلة • خوادم الوصول عن بُعد • أجهزة المستخدمين • الأجهزة المحمولة Malware protection solutions shall be configured to protect the endpoints of <entity name>'s information and technology assets, including: • Firewalls • Email servers • Web servers • Proxy servers • Remote-access servers • Workstations

• Mobile devices	
يجب أن تتمتع تقنيات وآليات الحماية من البرمجيات الضارة بلوحة تحكم مركزية، مما يضمن التطبيق المتسق لسياسة الحماية من البرمجيات الضارة على جميع الأجهزة ومراقبة تهديدات هذه البرمجيات الضارة. Malware protection solutions shall have a central console. This will ensure a consistent implementation of Malware Protection Policy across all endpoints, and continuous monitoring of malware threat.	4-1
يجب أن تتكون تقنيات وآليات الحماية من البرمجيات الضارة من واحدة أو أكثر من الأدوات التي تؤدي وظائف كل من: • برامج مكافحة الفيروسات • نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات • جدار الحماية • تصفية/فحص المحتوى • السماح بقائمة محددة من التطبيقات يجب أن تُحدد وظائف تقنيات وآليات الحماية من البرمجيات الضارة بناءً على مخرجات عملية تقييم المخاطر. Malware protection solution shall be comprised of one or multiple tools that provide the functions of: • Antivirus Software • Intrusion Prevention System • Firewall • Content Filtering/Scanning • Application Whitelisting The functions of malware protection solutions shall be determined based on the outcomes of the risk assessment process.	5-1
يجب 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. Malware detection and prevention events shall be sent to the central malware protection solution and to the central event	6-1

	and log management solution for analysis, correlation and decision-making.
7-1	يجب 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. • الفصل بين استخدامات المتصفح للتطبيقات المؤسسية وغير المؤسسية. • 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). Malware defensive mechanisms shall be also implemented to reduce the impact of malware threats if they occur. Those mechanisms include: • BIOS protection. • Application sandboxing. • Browser segregation for corporate and non-corporate applications. • Segregation through virtualization. • Restriction of the automatic activation of a downloaded file, shareware or freeware. • Restriction of end user's privileges on the device they use (without administrative rights). • Restriction of the automatic activation or use of macro files. • Denial of booting systems from diskettes or CDs except in case of an emergency and when using verified media.

	• Configuration of all software to warn the user in case documents with macros are opened.
8-1	يجب أن يكون إجراء إزالة تثبيت برنامج تقنيات وآليات الحماية من البرمجيات الضارة محمياً بكلمة مرور وتتم إدارته عن بعد لضمان عدم قدرة المستخدم على إزالة تثبيت البرنامج أو تغيير إعداداته أو إلغاء تفعيله. Uninstallation of a malware protection solution's agent shall be password protected and remotely managed to ensure that end users are unable to uninstall the agent, change its settings, or deactivate it.
2	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.
الإجراءات المطلوبة	
1-2	يجب ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة لإجراء فحص مباشر لجميع الملفات عند الوصول إليها أو نسخها أو نقلها لضمان اكتشاف جميع البرمجيات الضارة قبل تنشيطها. The malware protection solution's agent shall be configured to perform a real time scan on all files when they are accessed, copied or transferred. This will ensure the detection of all malware before activation.
2-2	يجب إعداد برنامج تقنيات وآليات الحماية من البرمجيات الضارة لإجراء فحص كامل للنظام أسبوعياً على الأقل، ويمكن أن يكون وقت الفحص عند تشغيل النظام أو خلال ساعات الاستخدام المنخفض. The malware protection solution's agent shall be configured to perform full system scan at least once a week. The time of scanning can be either when the system boots up or during non-peak usage hours.

3-2	تمكين خاصية فحص مكافحة البرمجيات الضارة للوسائط القابلة للإزالة عند إدخالها أو توصيلها. Anti-malware scanning shall be enabled for removable media when they are inserted or connected.
4-2	ضبط وإعداد الأجهزة بصورة تمنع التشغيل التلقائي للمحتوى. Devices shall be configured to not auto-run content.
5-2	تفعيل خاصية تسجيل استعلامات نظام أسماء النطاقات (DNS) للكشف عن الاستعلامات الخاصة بنطاقات نظام أسماء النطاقات (DNS) الضارة المعروفة. DNS query logging shall be enabled to detect queries for known malicious DNS domains.
6-2	تفعيل ميزات مكافحة الاستغلال على نظام التشغيل لاكتشاف و/أو منع الأنشطة المشبوهة والضارة. Operating system anti-exploitation features shall be enabled to detect and/or prevent suspicious and malicious activities.
7-2	يجب ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة لاكتشاف البرمجيات الضارة أولاً ثم الاستجابة لها على النحو التالي: تطهير البرمجيات الضارة، أو حذفها، أو عزلها أو تشفيرها. يجب أن يكون التشفير قابلاً للفك في حالة الاكتشاف الخاطئ لإحدى البرمجيات الضارة. The malware protection solution shall be configured to firstly detect then respond to the malware as follows: disinfect, delete, quarantine or encrypt malware upon detection. Encryption of the malware shall be reversible in the case of false positive detection.
8-2	ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة بحيث يقوم بعزل الملفات التي أصابها الفيروس في حال عدم القدرة على حذفها. The malware protection solution's agent shall be configured to quarantine virus-infected files if they cannot be cleaned.
9-2	ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة بحيث يقوم بتنبيه المستخدم بعدم قدرته على تنظيف أو عزل الشفرة الخبيثة.

The malware protection solution's agent shall be configured to notify the user if it is unable to clean or quarantine the malicious code detected on the machine.	
تنصيب 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. Malware protection solutions shall be installed on email servers including SMTP gateway. Malware protection solutions shall be configured to scan email content and attachments in all emails. If malware is found in an incoming SMTP mail, then the following actions shall be taken: • Infected attachments shall be cleaned. • Infected attachments shall be quarantined if cleaning them was not possible.	10-2
ضبط إعدادات نظام التشغيل والتطبيقات على لوحة التحكم المركزية بتقنيات وآليات الحماية من البرمجيات الضارة وفقاً لإرشادات الإعداد الآمن التي يوفرها المورد. Operating system and applications on the malware protection solution's central console shall be configured as per the relevant vendor's secure configuration guidelines.	11-2
منع الوصول إلى المواقع الإلكترونية والمصادر الأخرى على الإنترنت والمعروفة باستضافتها لمحتوى خبيث باستخدام آلية تصفية محتوى الويب. Access to websites and other resources on the Internet known to host malicious content shall be prevented using a web content filtering mechanism.	12-2
تقوم <اسم الجهة> بمراقبة الأداء للمعايير التالية: • استخدام وحدة التحكم المركزية (CPU) • استخدام الذاكرة • أداء الشبكة	13-2

	• استخدام القرص <Entity name> shall carry out performance monitoring for the following parameters: • CPU Utilization • Memory Utilization • Network Performance • Disk Utilization
14-2	يجب أن يقدم مشرفو تقنيات وآليات الحماية من البرمجيات الضارة تقاريراً 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. • أهم 10 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. Malware protection solutions' administrators shall submit periodic reports on a monthly basis on the status of malware protection to <entity name>'s <Cybersecurity Department>. The report shall include the following at a minimum: • Number of PCs, servers, laptops and systems not updated with the latest signature patterns. • Top 10 detected malware. • Number of viruses/worms/malicious programs detected. • Number of viruses/worms/malicious programs cleaned/quarantined/deleted. • Action taken to resolve the malware infection. • Source of infection.

3	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.
الإجراءات المطلوبة	
1-3	يجب تحديث تقنيات وآليات الحماية من البرمجيات الضارة بشكل مستمر وتلقائي وفقاً لسياسة إدارة التحديثات والإصلاحات. Malware protection solutions shall be automatically updated on a regular basis as per Patch Management Policy.
2-3	يجب التحقق من سلامة المعلومات والملفات الخاصة بتقنيات وآليات الحماية من البرمجيات الضارة دورياً. Malware protection solutions shall be periodically verified for integrity.
3-3	يجب تحديث قاعدة بيانات تواقيع تقنيات وآليات الحماية من البرمجيات الضارة تلقائياً أو يدوياً بشكل منتظم. Malware protection solutions' signature database shall be automatically or manually updated on a regular basis.
4-3	يجب إعداد تقنيات وآليات الحماية من البرمجيات الضارة للحصول على نمط التواقيع من الموقع الإلكتروني للمورد. Malware protection solutions shall be configured to acquire the signature pattern from the trusted vendor’s website.
5-3	يجب إعداد تقنيات وآليات الحماية من البرمجيات الضارة "لتوزيع" آخر تحديثات التواقيع على أجهزة المستخدمين والخوادم. Malware protection solutions shall be configured to “push” the latest signature updates to all workstations and servers.

6-3	يجب ضبط إعدادات الأجهزة غير الموجودة ضمن شبكة الأجهزة المحمولة في <اسم الجهة> لتتضمن خيارات تحديث بديلة بحيث يمكن تحديث التواقيع مباشرة من الموقع الإلكتروني للمورد. Systems which are not on <entity name>'s mobile device network shall be configured with alternative update options whereby the signatures can be directly updated from the vendor's website.
7-3	يجب 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. Malware protection solutions shall support signature update rollback in case the current latest updates make the antivirus software inconsistent and incapable of operating as expected.
4	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.
الإجراءات المطلوبة	
1-4	يجب 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 بـ<اسم الجهة> وما هي طريقة وصوله إليها). <Entity name> shall keep track of new threats arising from malicious code and shall maintain a list of the possible infection scenarios (e.g., how and in what way the virus can affect <entity name>'s information and technology assets).
2-4	يجب تحديد السيناريوهات بوضوح ويجب أن تتصدى تقنيات الحماية من البرمجيات الضارة لهذه البرمجيات وتتخلص منها على كافة المستويات.

Scenarios shall be clearly identified, and the malware protection solution shall fight and remove malware on all levels.	
عند وجود ثغرات جديدة، يجب أن تحدد <اسم الجهة> الخطوات التي يجب اتخاذها لضمان الحد من المخاطر المحتملة. When a new vulnerability is published, <entity name> shall identify the steps that need to be taken to ensure that the associated risks are mitigated.	3-4

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

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

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

الالتزام بالمعيار

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذا المعيار دورياً.

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

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