هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. والبنود الملوّنة باللون الأخضر هي أمثلة يجب حذفها. ويجب إزالة التظليل الملوّن بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج معيار إدارة التحديثات والإصلاحات

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 <1.0>

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 <1.0>

قائمة المحتويات

الغرض 4
نطاق العمل 4
المعايير 4
الأدوار والمسؤوليات 12
التحديث والمراجعة 12
الالتزام بالمعيار 12

الغرض

إن قدرة <اسم الجهة> على إدارة التصحيحات وفقًا لهذا المعيار ستساعد في تقليل مخاطر الأمن السيبراني، و ضمان الحماية من التهديدات الداخلية والخارجية ذات الصلة، وفي الحفاظ على توافر وسلامة وسرية أصول ومعلومات <اسم الجهة>.

تمت مواءمة هذا المعيار مع الضوابط والمعايير الصادرة عن الهيئة الوطنية للأمن السيبراني، بما في ذلك الضوابط الأساسية للأمن السيبراني (ECC-1:2018)، وضوابط الأمن السيبراني للبيانات (DCC-1:2022)، وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019)، وضوابط الأمن السيبراني للحوسبة السحابية (CCC-1:2020) والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

يغطي هذا المعيار جميع الأصول المعلوماتية والتقنية لدى <اسم الجهة> وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

1	خطة الاستجابة للمخاطر (Plan risk response)
الهدف	ضمان قيام الجهة بإدارة حزم التحديثات والإصلاحات وفقًا لتقييم مخاطر وثغرات الأمن السيبراني الواردة.
المخاطر المحتملة	تزداد احتمالية وجود ثغرات دون معالجة، في حالة عدم إجراء تحديثات وإصلاحات في ضوء عمليات إدارة الثغرات والمخاطر العامة لدى <اسم الجهة> (مثل إجراؤها فقط كمهمة تشغيلية).
الإجراءات المطلوبة	
1-1	أن تراعي <اسم الجهة> كل ثغرة أمنية في كل برنامج جديد تؤثر على أصول <اسم الجهة>، بما في ذلك التطبيقات، والأنظمة التشغيلية، وجدار الحماية.
2-1	أن تتجنب <اسم الجهة> مخاطر الأمن السيبراني التي من الممكن أن تنجم عن عدم توافر أو تقديم التحديثات والإصلاحات، مما يضمن تقليل احتمالية وقوع المخاطر من خلال القضاء على ظهور الهجمات: • إزالة تثبيت البرامج التي تحتوي على ثغرات • قطع الاتصال عن الأصول التي تحتوي على ثغرات • إيقاف تشغيل الأجهزة التي تعاني من ثغرات • تعطيل قدرات الحوسبة في الأجهزة القادرة على العمل بدونها.

3-1	أن تقوم <اسم الجهة> بالتخفيف من حدة مخاطر الأمن السيبراني من خلال إجراء التحديثات والإصلاحات بهدف التخلص من الثغرات، مثل: • تحديث وإصلاح البرامج التي تحتوي على ثغرات؛ • تعطيل الخصائص التي تحتوي على ثغرات • الترقية إلى نسخة البرنامج الأحدث التي لا تحتوي على ثغرات
4-1	أن تقوم <اسم الجهة> بتثبيت ضوابط أمنية إضافية للحد من استغلال الثغرات، مثل: • استخدام جدران الحماية وتصنيف الشبكات لعزل الأجهزة التي تعاني من ثغرات، وبالتالي الحد من ظهور الهجمات.
5-1	أن تحدد <اسم الجهة> السيناريوهات التالية على الأقل للاستجابة لمخاطر ثغرات البرامج والتي يجب إعدادها للتعامل مع هذه المخاطر: • حزم التحديثات والإصلاحات الروتينية (إجراءات قياسية للتحديثات والإصلاحات المتاحة ضمن دورة إصدار منتظمة) • التحديثات والإصلاحات الطارئة (لمعالجة الحالات الطارئة للتحديثات والإصلاحات في حالة الأزمات) • الحلول البديلة في حالات الطوارئ (للتخفيف مؤقتًا من الثغرات الأمنية قبل توفر التحديثات والإصلاحات) • الأصول غير القابلة للتحديث والإصلاح (العزل أو اتباع طرق أخرى للتخفيف من حدة مخاطر الأنظمة التي يتعذر تحديثها وإصلاحها بسهولة)
6-1	أن تحدد <اسم الجهة> مجموعات الصيانة وأن تضع خطة صيانة لكل مجموعة صيانة لكل سيناريو قابل للتنفيذ للاستجابة للمخاطر، مثل: • <خطط الصيانة للسيناريو الأول، حزم التحديثات والإصلاحات الروتينية> ○ يجب أن تتبنى <اسم الجهة> عمليات النشر المرحلية لحزم التحديثات والإصلاحات الروتينية حيث يتم بالبداية تحديث وإصلاح مجموعة فرعية صغيرة من الأصول المطلوب تحديثها وإصلاحها. • <خطط الصيانة للسيناريو الثاني، التحديثات والإصلاحات في حالات الطوارئ> ○ يجب أن تتبع <اسم الجهة> نهجًا عامًا لحزم التحديثات والإصلاحات في الحالات الطارئة مماثلاً لحزم التحديثات والإصلاحات الروتينية، باستثناء فيما يتعلق بجدول زمني متسارع للغاية. • <خطط الصيانة للسيناريو الثالث، الحلول البديلة في الحالات الطارئة> ○ يجب أن تخطط <اسم الجهة> لتنفيذ أنواع متعددة من الحلول البديلة للحالات الطارئة بشكل سريع لحماية الأصول التي تحتوي على ثغرات. • <خطط الصيانة للسيناريو الرابع، الأصول غير قابلة للتحديث والإصلاح> ○ يجب أن تخطط <اسم الجهة> لتنفيذ العديد من أنواع طرق التخفيف من حدة المخاطر على المدى الطويل إلى جانب حزم التحديثات والإصلاحات لحماية الأصول التي تحتوي على ثغرات.

اختر التصنيف

الإصدار <1.0>

2	تنفيذ الاستجابة للمخاطر (Execute risk response)
الهدف	التأكد من تنفيذ حزم التحديثات والإصلاحات باتباع نهج منظم بشكل منطقي لتنفيذ الاستجابة للمخاطر.
المخاطر المحتملة	من الممكن أن يفشل تقييم المخاطر في العديد من الحالات، في حالة عدم تنفيذ استجابة مصممة أو منظمة جيدًا للمخاطر، الأمر الذي قد يؤدي إلى وجود ثغرات بدون تحديثات أو إصلاحات أو معالجة.
الإجراءات المطلوبة	
1-2	أن يتكون تنفيذ الاستجابة للمخاطر من الخطوات التالية: ● إعداد الاستجابة للمخاطر ● تنفيذ الاستجابة للمخاطر ● التحقق من الاستجابة للمخاطر ● مراقبة الاستجابة للمخاطر بشكل مستمر
2-2	أن يغطي إعداد الاستجابة للمخاطر الأنشطة التالية: ● الحصول على حزم التحديثات والإصلاحات ● التحقق من حزم التحديثات والإصلاحات ● اختبار حزم التحديثات والإصلاحات
3-2	أن يغطي تنفيذ الاستجابة للمخاطر الأنشطة التالية: ● تطبيق عمليات إدارة التغيير ● تحديد طريقة التثبيت ● تحديد أولويات وجدولة حزم التثبيت
4-2	أن يغطي التحقق من الاستجابة للمخاطر الأنشطة التالية: ● تأكيد حزم التحديثات والإصلاحات المثبتة ● التحقق من مدى فعالية حزم التحديثات والإصلاحات ○ فحص الثغرات ○ استخدام المقاييس (مؤشرات الأداء الرئيسية)
5-2	أن تغطي المراقبة المستمرة للاستجابة للمخاطر الأنشطة التالية: ● التأكد من عدم قيام أي شخص بإلغاء تثبيت حزم التحديثات والإصلاحات ● التأكد من عدم استعادة النسخة الأقدم من البرنامج المحدّث

اختر التصنيف

الإصدار <1.0>

	• تقييم الثغرات الدوري لحزم التحديثات والإصلاحات المثبتة
3	إعداد الاستجابة للمخاطر (Prepare risk response)
الهدف	الحصول على حزم التحديثات والإصلاحات والتحقق منها واختبارها للبرامج التي تحتوي على ثغرات أو تطبيق ضوابط أمنية إضافية لحماية تلك البرامج.
المخاطر المحتملة	التحقق: يمكن الحصول على حزمة التحديثات والإصلاحات من مصادر مخادعة أو تم العبث بها خلال النقل أو بعد الحصول عليها. الاختبار: المخاطر التشغيلية من خلال تحديد المشاكل التي تحتوي عليها حزمة التحديثات والإصلاحات قبل تفعيلها.
الإجراءات المطلوبة	
1-3	الحصول على حزم التحديثات والإصلاحات فقط من مصادر مشروعة وموثوقة. ويتضمن ذلك الحصول عليها من مواقع آمنة يوفرها المورد/ المصنّع أو يتم تطويرها داخليًا.
2-3	مراقبة حزمة التحديثات والإصلاحات المتاحة من قبل مالك الأصول وتثبيتها إذا كانت مفيدة تقنيًا، ووفقًا لمستوى حساسية الأصول المحدثة، وبعد اختبار حزمة التحديثات والإصلاحات.
3-3	التأكيد على سلامة الملف قبل اختبار حزمة التحديثات والإصلاحات أو تثبيتها باستخدام خوارزميات التجزئة إذا كانت مفيدة تقنيًا (مثل: جدار الحماية على أجهزة الشبكة).
4-3	إجراء فحص فيروسات بشكل دوري على حزم التحديثات والإصلاحات التي تم تحميلها، لتجنب تثبيت البرمجيات الضارة.
5-3	اختبار حزم التحديثات والإصلاحات قبل تثبيتها أو تفعيلها بشكل مباشر.
6-3	في حالة التحديثات والإصلاحات اللازمة للبرامج، يجب استخدام بيئة اختبار منفصلة بهدف تجنب مشاكل عدم توافق الأنظمة أو الإصابة بالفيروسات.
7-3	توثيق المشاكل المستقبلية وحلّها في مرحلة الاختبار قبل التفعيل المباشر لحزم التحديثات والإصلاحات.
8-3	تفعيل العمليات بخيار الاسترجاع في حال وجود حالة عدم توافق غير متوقعة، بحيث يمكن استعادة الأنظمة لحالة ما قبل التحديث والإصلاح.

9-3	تنفيذ وظائف النسخ الاحتياطي والاستعادة في حال ظهور حالة عدم توافق غير متوقعة، ليتم التأكد من توفر النظام في مثل هذه الحالات.
4	تنفيذ الاستجابة للمخاطر (Implement risk response)
الهدف	التأكد من سلامة واستمرارية نظام المعلومات من خلال توزيع حزم التحديثات والإصلاحات وتثبيتها وإعدادات الأصول وحالتها.
المخاطر المحتملة	إدارة التغيير: قد يؤدي تطبيق حزم التحديثات والإصلاحات بدون عملية إدارة تغيير مناسبة إلى وقف عمليات الجهة أو حتى فقدان البيانات. تحديد الأولويات والجدولة: بدون تحديد أولويات حزم التحديثات والإصلاحات، هناك احتمال ألّا يتم تثبيت بعض حزم التحديثات والإصلاحات الحرجة أو عالية الخطورة بأحد الأصول المهمة.
الإجراءات المطلوبة	
1-4	جدولة عمليات تثبيت حزم التحديثات والإصلاحات في إطار نشاط إدارة التغيير لدى <اسم الجهة>.
2-4	أن تقوم <اسم الجهة> بتطبيق تلك التغييرات فقط على البيئة الحيّة لدى <اسم الجهة> التي تم اعتمادها من خلال إجراءات إدارة التغيير في <اسم الجهة>.
3-4	توثيق إجراءات تطبيق حزمة التحديثات والإصلاحات المثبتة بهدف تتبعها (مثل الموافقة والاختبار الذي تم بالفعل).
4-4	استخدام طرق تثبيت حزم التحديثات والإصلاحات التالية: ● توزيع حزم التحديثات والإصلاحات من خلال حلول مركزية ○ استخدام التثبيت التلقائي ○ جدولة تثبيت حزم التحديثات والإصلاحات ○ تثبيتها يدويًا (التثبيت الإجباري) ● تثبيت حزم التحديثات والإصلاحات كعملية واحدة
5-4	تحديد أولويات حزم التحديثات والإصلاحات بهدف البدء بتثبيت الحزم ذات الأولوية الأعلى، وفقًا لنتائج تقييم المخاطر لدى <اسم الجهة>
6-4	أن يستند تحديد أولويات حزم التحديثات والإصلاحات إلى أهمية الأصول، ووفقًا لسياسة ومعيار إدارة الثغرات. يجب أن تقوم <اسم الجهة> بإعداد مقياس ملخص وقت التخفيف من الثغرات (الجدول 1 في الملحق) وتقديم مقاييس التخفيف بناءً على ما يلي: ● الأهمية النسبية للأصول (منخفض، ومتوسط، ومرتفع) وفقًا للتصنيف في <اسم الجهة> .

اختر التصنيف

الإصدار <1.0>

	• الثغرات (منخفض، متوسط، ومرتفع، وحرج)، وفقًا لتصنيف <اسم الجهة> والمتطلبات التشريعية والتنظيمية الصادرة.
5	التحقق من الاستجابة للمخاطر ومراقبتها (Verify and monitor risk (response
الهدف	التأكد من استكمال التنفيذ بنجاح. يعني ذلك بالنسبة لحزم التحديثات والإصلاحات التأكيد على تثبيت الحزم وتفعيلها، وضمان عملها على النحو المنشود بالنسبة للضوابط الأمنية الإضافية.
المخاطر المحتملة	في حال عدم مراقبة أو تأكيد تثبيت حزم التحديثات والإصلاحات، فهنالك مخاطر أن تبقى أصول المعلومات تعاني من الثغرات وعرضة للهجمات.
الإجراءات المطلوبة	
1-5	التحقق من فعالية حزم التحديثات والإصلاحات بهدف التحقق من نجاحها. ويجب استخدام التقنيات التالية لغايات التحقق: • إجراء فحص الثغرات حول الأصول المزودة بحزم التحديثات والإصلاحات • استخدام المقاييس (مؤشرات الأداء الرئيسية) المقدمة من أنظمة المعلومات والتي أُستخدمت لتثبيت حزم التحديثات والإصلاحات (WSUS, HPSA, SCCM)
2-5	مراقبة الاستجابة للمخاطر بشكل مستمر، مع مراعاة الأمور التالية: • يجب تثبيت حزم التحديثات والإصلاحات فقط من قبل الموظفين المختصين (قسم عمليات تقنية المعلومات). يجب تعطيل جميع وسائل التثبيت الأخرى من قبل مسؤول النظام. • يجب أن تتأكد <اسم الجهة> من عدم قيام أي شخص بإلغاء تثبيت حزمة التحديثات والإصلاحات، أو إلغاء تفعيل ضوابط الأمن الإضافية، أو السماح بانتهاء تأمين الأمن السيبراني، أو إعادة تشغيل الجهاز الذي تم إيقاف تشغيله.
6	معايير أخرى (Other Standards)
الهدف	تثبيت إدارة حزم التحديثات والإصلاحات بشكل آمن واستخدامها بشكل مناسب عند الحاجة.
المخاطر المحتملة	قد تتعرض <اسم الجهة>، في حال عدم امتثالها للمعايير والمتطلبات، إلى تهديدات خطيرة.
الإجراءات المطلوبة	
1-6	يجب تنفيذ المعايير فيما يتعلق بإدارة حزم التحديثات: 1- سياسة إدارة الثغرات

	2- معيار إدارة الثغرات 3- سياسة إدارة مخاطر الأمن السيبراني

الجدول 1 -مصفوفة ملخص وقت التخفيف من الثغرات <مع نموذج للبيانات>

أهمية الثغرات	أهمية الأصول		
	منخفضة	متوسطة	مرتفعة
منخفضة	بحلول الموعد النهائي: 64.7 % متوسط الوقت: 80.4 يومًا معدل الوقت: 75.2 يوماً	بحلول الموعد النهائي: 72.4 % متوسط الوقت: 34.7 يومًا معدل الوقت: 33.7 يومًا	بحلول الموعد النهائي: 85.0% متوسط الوقت: 14.6 يومًا معدل الوقت: 8.1 يومًا
متوسطة	بحلول الموعد النهائي: 66.5 % متوسط الوقت: 75.1 يومًا معدل الوقت: 70.7 يومًا	بحلول الموعد النهائي: 68.7 % متوسط الوقت: 33.2 يومًا معدل الوقت: 31.6 يومًا	بحلول الموعد النهائي: 71.4 % متوسط الوقت: 12.9 يومًا معدل الوقت: 10.5 يومًا
مرتفعة	بحلول الموعد النهائي: 68.6 % متوسط الوقت: 62.1 يومًا معدل الوقت: 58.0 يومًا	بحلول الموعد النهائي: 78.8 % متوسط الوقت: 26.8 يومًا معدل الوقت: 22.1 يومًا	بحلول الموعد النهائي: 85.5 % متوسط الوقت: 8.8 يومًا معدل الوقت: 8.1 يومًا
حرجة	بحلول الموعد النهائي: 81.4 % متوسط الوقت: 44.4 يومًا	بحلول الموعد النهائي: 92.3 % متوسط الوقت: 21.2 يومًا معدل الوقت: 23.9 يومًا	بحلول الموعد النهائي: 95.2 % متوسط الوقت: 5.2 يومًا معدل الوقت: 5.1 يومًا

اختر التصنيف

الإصدار <1.0>

	معدل الوقت: 41.3 يومًا		

تعكس المقاييس في كل خلية النسبة المئوية للأصول التي تم تزويدها بحزم التحديثات والإصلاحات من خلال المواعيد النهائية لخطط الصيانة المقابلة، بالإضافة إلى متوسط الوقت (المتوسط) ومعدل الوقت لحزم التحديثات والاصلاحات.

الأدوار والمسؤوليات

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

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

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

4- **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

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

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>.