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 إدارة الثغرات

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.

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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	عُدلَ 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

يهدف هذا المعيار إلى تحديد متطلبات الأمن السيبراني التفصيلية لضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع أو تقليل احتمالية استغلال هذه الثغرات من خلال الهجمات السيبرانية، والتقليل من الآثار الناتجة عن هذه الهجمات على أعمال <اسم الجهة>، وحمايتها من التهديدات الداخلية والخارجية في <اسم الجهة>. هذه المتطلبات تمت موائمتها مع سياسة إدارة الثغرات ومتطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني ويشمل ذلك على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – ١: ٢٠١٨)، ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – ١: ٢٠١٩) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق المعيار

يطبق هذا المعيار على جميع الأصول المعلوماتية والتقنية في <اسم الجهة>، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

١	المتطلبات العامة
الهدف	تحديد المتطلبات العامة لتقييم الثغرات التي يجب أن يتبعها فريق تقييم الثغرات الداخلي أو الخارجي قبل بدء عملية تقييم الثغرات.
المخاطر المحتملة	يمكن أن يؤدي تقييم الثغرات غير المخطط له بشكل صحيح إلى مخرجات غير كافية أو غير دقيقة، أو قد تؤثر عملية تقييم الثغرات على كفاءة الأنظمة والخدمات.
الإجراءات المطلوبة	
١-١	إعداد خطة لتقييم الثغرات بشكل دوري يوضح فيها نطاق العمل وتاريخ البدء والانتهاء.
١-٢	التأكد من أن خطة تقييم الثغرات متوافقة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.
١-٣	التأكد من أن نشاط إدارة الثغرات (والذي يشمل الاكتشاف والفحص والتصنيف والمعالجة) يسير وفقاً لمنهجية محددة ووفقاً لنماذج سياسات وإجراءات وعمليات إدارة مخاطر الأمن السيبراني والمخاطر المؤسسية المعتمدة في <اسم الجهة>.
١-٤	إعداد تقرير بعد الانتهاء من أنشطة تقييم الثغرات على أن يتضمن التقرير الأقسام التالية على الأقل: • الملخص التنفيذي.

اختر التصنيف

الإصدار <١,٠>

	• مقدمة لإعداد التقارير. • المنهجية. • الأصول المستهدفة. • تقرير تفصيلي لنتائج تقييم الثغرات.
١-٥	بعد الانتهاء من تقرير تقييم الثغرات، يجب إعداد خطة عمل لتنفيذ التوصيات، على أن يتضمن التقرير ما يلي على الأقل: • المسؤول التقني عن الأصل (Technical Owner). • مالك الأصل (Business Owner). • الإجراءات المطلوبة لتنفيذ التوصيات. • الفترة الزمنية اللازمة لتنفيذ التوصيات.
٢	آلية تقييم الثغرات
الهدف	تحديد ووضع خطة لوسائل تقييم الثغرات والأدوات المستخدمة التي يجب أن يتبعها فريق تقييم الثغرات الداخلي أو الخارجي قبل بدء عملية تقييم الثغرات.
المخاطر المحتملة	قد يؤدي تقييم الثغرات من غير آلية واضحة ومعتمدة إلى نتائج غير واضحة أو غير دقيقة، وبالتالي قد تُستغل تلك الثغرات قبل اكتشافها وأيضاً قد تتسبب بإهدار الموارد والوقت.
الإجراءات المطلوبة	
١-٢	إجراء تقييم الثغرات دورياً أو مرة واحدة في السنة على الأقل.
٢-٢	إجراء تقييم الثغرات مرة واحدة شهرياً للمكونات التقنية للأنظمة الحساسة الخارجية.
٣-٢	إجراء تقييم الثغرات مرة واحدة كل ثلاثة أشهر للمكونات التقنية للأنظمة الحساسة الداخلية.
٤-٢	تقييم ومعالجة الثغرات الخاصة بأنظمة العمل عن بعد وتصنيفها حسب خطورتها، مرة واحدة كل ثلاثة أشهر على الأقل.
٥-٢	تقييم ومعالجة الثغرات الخاصة بالخدمات السحابية مرة واحدة كل ثلاثة أشهر على الأقل.
٦-٢	التأكد من تنفيذ تقييم الثغرات وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، مع الأخذ بالاعتبار الإرشادات التالية:

	• توفير المتطلبات الخاصة ببدء فحص واكتشاف الثغرات الواردة في إجراءات إدارة الثغرات. • تحديد المكونات التقنية المستهدفة بالفحص وتوفير الصلاحيات اللازمة للقيام بفحص واكتشاف الثغرات. • التأكد من أن عملية فحص واكتشاف الثغرات تغطي ثغرات الشبكة وثغرات الخدمات والرسائل النصية التعريفية (Banner Grabbing). • إجراء فحص واكتشاف ثغرات عن طريق وسائل وتقنيات معتمدة. • تحصين أدوات اكتشاف الثغرات الأمنية لمنع الاستخدام أو التعديل غير المصرح به، ومنع تغيير إعداداتها. في حال كان تغيير الإعدادات مطلوبًا، فيجب اتباع إجراءات إدارة التغيير والحصول على الموافقات اللازمة من قبل <اسم الجهة>. • تصنيف تقارير تقييم الثغرات الأمنية بتصنيف "سري" على الأقل وحمايتها بكلمة مرور ومشاركتها فقط مع الجهات ذات العلاقة. • تصنيف الثغرات حسب خطورتها ووفقاً لمنهجية إدارة المخاطر السيبرانية.
٣	معالجة الثغرات
الهدف	تحديد آلية لمعالجة الثغرات بشكل فعّال ومنع أو تقليل احتمالية استغلال هذه الثغرات، وتقليل الآثار الناتجة عن هذه الهجمات على سير الأعمال.
المخاطر المحتملة	قد يؤدي عدم معالجة الثغرات إلى استغلال تلك الثغرات واستخدامها لشن هجمات سيبرانية.
الإجراءات المطلوبة	
١-٣	إعداد خطة لمعالجة الثغرات على المكونات التقنية المستهدفة توضح فيها تفاصيل الثغرات والتوصيات وتاريخ البدء وتاريخ الانتهاء والإدارات/المشرفين المعنيين بمعالجة الثغرات.
٢-٣	توثيق خطة العمل واعتمادها من قبل <اسم الجهة>.
٣-٣	أن تكون جميع المكونات التقنية لدى <اسم الجهة> مضمونة ومدعومة من قبل المورد/المصنّع وفقاً لاتفاقية مستوى الخدمة مع المورد/المصنّع.
٤-٣	أن تكون لجميع المكونات التقنية الموجودة لدى <اسم الجهة> حزم تحديثات وإصلاحات أمنية محدثة على مستوى نظام التشغيل والتطبيقات.

٣-٥	يفضل أن يتم توفير تقنيات أتمتة (إن وجدت) لتحديثات أنظمة التشغيل والبرامج (بما في ذلك برامج الأطراف الخارجية) داخل <اسم الجهة>.
٣-٦	يجب معالجة الثغرات الحرجة (Critical Vulnerabilities) فور اكتشافها ووفقاً لآليات إدارة التغيير المعتمدة لدى <اسم الجهة>. ينبغي أن تكون لجميع الثغرات التي تشكل مخاطر مرتفعة أو متوسطة خطة عمل لإغلاقها ومعالجتها خلال أسبوعين كحد أقصى من تاريخ إصدار الإصلاح أو حزمة التحديثات والإصلاحات من قبل المورد، إلا إذا كان هناك مبرر تقني أو مبرر بناءً على احتياجات العمل يمنع ذلك وتم التبليغ عنه رسمياً.
٣-٧	الثغرات التي تم إشعار <اسم الجهة> بها عن طريق مقدم خدمات الحوسبة السحابية ومعالجتها.

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>.

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

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا على الأقل أو في حال 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 دورياً.

٢- يجب على جميع 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>.