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:

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

اختر التصنيف

الإصدار 1.0

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير 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 من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

يهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-١٠-١ 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 في <اسم الجهة>، وينطبق على جميع العاملين في <اسم الجهة>.

المعايير

1	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	
1-1	يجب إعداد خطة لتقييم الثغرات يوضح فيها نطاق العمل وتاريخ البدء والانتهاء. A plan for vulnerability assessment that covers the assessment scope, start date, and end date shall be developed.
2-1	يجب التأكد من أن خطة تقييم الثغرات متوافقة مع المتطلبات التشريعية والتنظيمية ذات العلاقة. Vulnerability assessment plan shall be based on the relevant legislative and regulatory requirements.

3-1	ينبغي 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>. Vulnerability management activity shall follow a defined methodology, in accordance with <entity name>'s enterprise and cybersecurity risk management policies, procedures, and processes.
4-1	ينبغي صياغة تقرير بعد الانتهاء من نشاط تقييم الثغرات. ويجب أن يتضمن التقرير الأقسام التالية على الأقل: • الملخص التنفيذي. • مقدمة لإعداد التقارير. • المنهجية. • الأصول المستهدفة. • تقرير تفصيلي لنتائج تقييم الثغرات. A report shall be developed after finalizing the vulnerability assessment activities. The report shall include the following sections at minimum: • Executive Summary • Reporting Introduction • Methodology • Target Assets • Detailed Findings
5-1	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.

	An action plan shall be developed after finalizing the vulnerability assessment report in order to implement the recommendations. The report shall have at minimum: • Technical Owner • Business Owner • Required Actions • Clear Deadlines
6-1	ينبغي مقارنة نتائج تقييم الثغرات مع النتائج السابقة للتأكد من معالجة الثغرات السابقة في الوقت المحدد. Results from previously conducted vulnerability scans and assessments shall be compared with current results to ensure that remediation actions have been implemented in a timely manner.
2	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	
1-2	يجب إجراء تقييم الثغرات دورياً أو مرة واحدة في السنة على الأقل. Vulnerability assessment shall be performed periodically or at least annually.
2-2	يجب إجراء تقييم الثغرات مرة واحدة شهرياً للمكونات التقنية للأنظمة الحساسة الخارجية. (CSCC-2-9-1-2) Vulnerability assessment shall be conducted on a monthly basis for all external critical systems (Internet-facing systems). (CSCC-2-9-1-2)
3-2	يجب إجراء تقييم الثغرات مرة واحدة كل ثلاثة أشهر للمكونات التقنية للأنظمة الحساسة الداخلية. (CSCC-2-9-1-2)

	Vulnerability assessment shall be conducted on a quarterly basis for all internal critical systems. (CSCC-2-9-1-2)
4-2	يجب التأكد من تنفيذ تقييم الثغرات وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، مع الأخذ بالاعتبار الإرشادات التالية: 2-4-1 توفير المتطلبات الخاصة ببدء فحص واكتشاف الثغرات الواردة في إجراءات إدارة الثغرات. 2-4-2 تحديد المكونات التقنية المستهدفة بالفحص وتوفير الصلاحيات اللازمة للقيام بفحص واكتشاف الثغرات. 2-4-3 التأكد من أن عملية فحص واكتشاف الثغرات تغطي ثغرات الشبكة وثغرات الخدمات والرسائل النصية التعريفية (Banner Grabbing). 2-4-4 إجراء فحص واكتشاف ثغرات عن طريق وسائل وتقنيات معتمدة. 2-4-5 تصنيف الثغرات حسب خطورتها ووفقاً لمنهجية إدارة المخاطر السيبرانية. Vulnerability assessment exercise shall be conducted as per the relevant legislative and regulatory requirements, and it shall take into account the following guidelines: 2-4-1 The exercise shall meet specific vulnerability assessment requirements which are mentioned in the procedures. 2-4-2 The exercise shall define the systems/applications targeted for assessment, as well as any targeted system/application specific requirements. 2-4-3 The assessment shall include network-related vulnerabilities, service-based vulnerabilities, and banner grabbing. 2-4-4 Vulnerability assessment shall be performed using approved methods and mechanisms. 2-4-5 Risk rating shall be determined to prioritize findings as per the cybersecurity risk management methodology.
3	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.

اختر التصنيف

الإجراءات المطلوبة	
1-3	يجب إعداد خطة لمعالجة الثغرات على المكونات التقنية المستهدفة توضح فيها تفاصيل الثغرات والتوصيات وتاريخ البدء وتاريخ الانتهاء والإدارات/المشرفين المعنيين بمعالجة الثغرات. An action plan for remediation, fixing the identified gaps and patching targeted systems/applications, shall be developed. The plan shall include vulnerabilities details, recommendations, assessment start date and end date, and the functions/teams involved in the exercise.
2-3	يجب توثيق خطة العمل واعتمادها من قبل <الإدارة المعنية بالأمن السيبراني>. The vulnerability assessment action plan shall be documented and approved by <Cybersecurity Department>.
3-3	يجب أن تكون جميع المكونات التقنية لدى <اسم الجهة> مضمونة ومدعومة من قبل المورد/المصنّع وفقاً لاتفاقية مستوى الخدمة مع المورد/المصنّع. All systems and devices within <entity name> shall have vendor/manufacturer warranty as per the Service Level Agreement with the vendor/manufacturer.
4-3	يجب أن تكون لجميع المكونات التقنية الموجودة لدى <اسم الجهة> حزم تحديثات وإصلاحات أمنية محدثة على مستوى نظام التشغيل والتطبيقات. All systems and devices within <entity name> should have up-to-date security patches at the operating system and application level.
5-3	من المستحسن أن يتم توفير تقنيات أتمتة (إن وجدت) تحديثات أنظمة التشغيل والبرامج (بما في ذلك برامج الأطراف الخارجية) داخل <اسم الجهة>. Automated tools for updating operating systems and software (including third party software) are encouraged to be deployed in the environment.
6-3	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. Critical vulnerabilities shall be patched immediately after their discovery as per <entity name> change management procedures. Any high or medium risk vulnerabilities should have a priority in the action plan, and be closed and remediated within a maximum of two weeks from releasing the fix or patch from the vendor, unless there is business or technical justification that is communicated officially.	

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>.