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 اختبار الاختراق

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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.

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 لاختبار وتقييم مدى فعالية قدرات تعزيز الأمن السيبراني في <اسم الجهة> وذلك من خلال محاكاة تقنيات الهجوم السيبراني وأساليبه الفعلية، واكتشاف نقاط الضعف الأمنية غير المعروفة التي قد تؤدي إلى الاختراق السيبراني لـ<اسم الجهة> 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، وهي مطلب تشريعي في الضابط رقم ٢-١١-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع أنظمة <اسم الجهة> الحساسة ومكوناتها التقنية، وجميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) ومكوناتها التقنية والتي تشمل البنية التحتية، والمواقع الإلكترونية، وتطبيقات الويب، وتطبيقات الهواتف الذكية واللوحية، والبريد الإلكتروني، والدخول عن بعد، وتنطبق هذه السياسة على جميع العاملين في <اسم الجهة>.

المعايير

1	المتطلبات العامة
الهدف	تحديد المتطلبات العامة لاختبار الاختراق (Penetration Testing) التي يجب أن يتبعها فريق اختبار الاختراق الداخلي أو الخارجي قبل بدء عملية اختبار الاختراق.
المخاطر المحتملة	يمكن أن يؤدي اختبار الاختراق غير المخطط له بشكل صحيح إلى مخرجات غير كافية أو غير دقيقة، أو قد يؤثر على كفاءة الأنظمة.
الإجراءات المطلوبة	
1-1	يجب تطوير خطة لاختبار الاختراق يوضح فيها نطاق العمل وتاريخ البدء والانتهاء وآلية وسيناريوهات تنفيذ عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية. A plan for penetration testing that covers in-scope systems and applications, start date, end date, methodology, and real-world attack scenarios shall be developed.
2-1	يجب التأكد من أن خطة العمل لاختبار الاختراق متوافقة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

	Penetration testing action plan shall be designed based on the relevant legislative and regulatory requirements.
3-1	يجب التأكد من أن اختبار الاختراق يسير وفقاً لمنهجية محددة ووفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. Penetration testing shall follow a defined methodology, conducted as per the relevant legislative and regulatory requirements
4-1	يجب صياغة وثيقة قواعد التنفيذ قبل البدء بالاختبار والتي تغطي نطاق الاختبار ومدته والأنظمة المستهدفة والبنود والشروط. Rules of engagement document shall be developed prior to the test, and it shall cover test scope, duration, target systems, and terms and conditions.
5-1	يجب إعداد تقرير لنتائج اختبار الاختراق يوضح تأثير المخاطر وآلية معالجتها والمسؤول عن تطبيقها والفترة الزمنية اللازمة لتنفيذها، على أن يتضمن التقرير الأقسام التالية على الأقل: • الملخص التنفيذي. • مقدمة لإعداد التقارير. • المنهجية المتبعة في تصنيف الثغرات. • الأصول المستهدفة، وسيناريوهات الهجمات (Attack Scenarios). • تقرير تفصيلي لنتائج اختبار الاختراق. A report shall be developed after finalizing the penetration testing activity. The report shall include the following sections at minimum: • Executive Summary • Reporting Introduction • Approach and Methodology • Target Assets and Attack Scenarios • Detailed Findings
6-1	بعد الانتهاء من تقرير اختبار الاختراق، يجب إعداد خطة عمل لتنفيذ التوصيات، على أن يتضمن التقرير ما يلي على الأقل:

اختر التصنيف

	• 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 penetration testing report in order to implement the recommendations. The report shall include the following at minimum: • Technical Owner • Business Owner • Required Actions • Clear Deadlines
7-1	يجب التأكد من أن تقنيات المستخدمين وأدواتهم وحساباتهم، وكذلك الأجهزة المستخدمة في اختبار الاختراق أو كانت جزءاً منه، خاضعة للتحكم والمراقبة وذلك لضمان استخدامها لغرض اختبار الاختراق فقط. Any user, system or workstation that was used in, or was part of, the penetration testing exercise shall be controlled and monitored to ensure that they are used only for the purpose of the testing exercise.
8-1	يجب تعطيل أو إزالة التقنيات والأدوات وحسابات المستخدمين بعد الانتهاء من عملية اختبار الاختراق. Any user, system or workstation that was used in, or was part of, the penetration testing exercise shall be removed or restored to normal behavior and access after the testing exercise.
9-1	يجب إعداد تقرير لكل اختبار اختراق غير ناجح أو غير مكتمل توضح فيه الصعوبات التي واجهت فريق الاختبار لدراسة العوائق وحلها وإعادة الاختبار مرة أخرى. A report shall be developed for each failed or incomplete penetration testing exercise. The report shall highlight the limitations faced by the test team to understand and resolve them, and redo the exercise.

2	آلية اختبار الاختراق
الهدف	تحديد آلية اختبار الاختراق والأدوات والتقنيات المستخدمة التي يجب أن يتبعها فريق اختبار الاختراق الداخلي أو الخارجي قبل بدء عملية اختبار الاختراق.
المخاطر المحتملة	يمكن أن يؤدي اختبار الاختراق غير المدروس إلى حصول ثغرات جديدة أو وصول غير مصرح به أو استمرار وجود نقاط ضعف أمنية في البيئة لا يتم اكتشافها مما يؤدي إلى نتائج غير دقيقة، كما يمكن أن يؤدي إلى تسرب البيانات أو كشفها أو إلحاق الضرر بالأنظمة والخدمات والمكونات التقنية.
الإجراءات المطلوبة	
1-2	يجب إجراء اختبار الاختراق دورياً. (ECC-2-11-3-2) Penetration testing shall be performed periodically.
2-2	يجب إجراء اختبار الاختراق لجميع الخدمات المقدمة خارجياً ومكوناتها التقنية دورياً وحسب جدول محدد ووفقاً لمنهجية وإجراءات محددة. (ECC-2-11-3-1) Penetration testing shall be conducted for all Internet-facing systems on a scheduled and regular basis, and following defined methodology and procedures. (ECC-2-11-3-1)
3-2	يجب إجراء اختبار الاختراق لجميع الأنظمة الحساسة ومكوناتها التقنية بانتظام وبحسب جدول محدد (كل 6 أشهر) ووفقاً لمنهجية وإجراءات محددة. (CSCC-2-10-1-1) Penetration testing shall be conducted for all critical systems on a scheduled and regular basis (every 6 months), and shall follow defined methodology and procedures. (CSCC-2-10-1-1)
4-2	يجب التأكد من تنفيذ اختبار الاختراق وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، مع الأخذ بالاعتبار الإرشادات التالية: 1-4-2 توفير المتطلبات الخاصة ببدء اختبار الاختراق الواردة في إجراءات اختبار الاختراق. 2-4-2 تحديد آلية الاختبار والتي تتضمن اختبار الصندوق الأسود (اختبار اختراق دون توفير معلومات للجهة التي تجري الاختبار)، واختبار الصندوق الأبيض (اختبار اختراق مع توفير جميع المعلومات للجهة التي تجري الاختبار)، واختبار الصندوق الرمادي (اختبار اختراق مع توفير بعض المعلومات للجهة التي تجري الاختبار). 3-4-2 تحديد الأنظمة أو الخدمات أو المكونات التقنية المستهدفة بالاختبار وأي معلومات أو صلاحيات يجب توفيرها قبل بدء اختبار الاختراق.

اختر التصنيف

4-4-2 الاطلاع على تقارير اختبارات الاختراق السابقة والمستندات المساعدة (إن وجدت) مثل مخططات الشبكة والمعايير التقنية الأمنية واستخدامها كمدخلات لعملية اختبار الاختراق لفهم طبيعة الأعمال للنظام أو التطبيق أو المكون التقني. 5-4-2 التأكد من عمل محاكاة لتقنيات الهجوم السيبراني وأساليبه الفعلية خلال عملية اختبار الاختراق تشمل بحد أدنى ما يلي: • الهندسة الاجتماعية. • اختبار الاختراق على مستوى الشبكة. • اختبار الاختراق على مستوى التطبيق. • اختبار الاختراق للشبكة اللاسلكية. • الدخول غير المصرح به. 6-4-2 إنشاء منصة أو بيئة تحاكي الأنظمة أو الخدمات المستهدفة باختبار الاختراق لعمل الاختبار عليها بدلاً من الأنظمة والخدمات الإنتاجية (أي الحقيقية). 7-4-2 توثيق النتائج لكل خطوة من خطوات اختبار الاختراق.	
Penetration testing exercise shall be conducted as per the relevant legislative and regulatory requirements and shall take into account the following guidelines: 2-4-1 The exercise shall meet specific penetration testing requirements, which are mentioned in the procedures. 2-4-2 The exercise shall define the testing approach (whether black box, white box, or grey box). 2-4-3 The systems/applications, services, or technical components targeted for testing shall be identified, as well as any system/application specific information, requirements or permissions targeted for testing. 2-4-4 Previous testing reports and supporting documents such as network diagrams and Technical Security Standards shall be reviewed and utilized as inputs for the testing exercise to understand how a system, application or technical component functions. 2-4-5 Simulation of real-world attack scenarios shall be conducted in the penetration testing and it shall include, at minimum, the following:	

• Social Engineering • Network Level Penetration Testing • Application Level Penetration Testing • Wireless Penetration Testing • Unauthorized Access 2-4-6 A test bed or an environment that mimics critical systems or production environment shall be created. 2-4-7 Results shall be documented for each step in the testing exercise.	

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>.