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 سياسة اختبار الاختراق

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

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير في تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في <اسم الجهة> وذلك من خلال محاكاة تقنيات وأساليب الهجوم السيبراني الفعلية، ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني لـ<اسم الجهة> من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة 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

تغطي هذه السياسة جميع الأنظمة الحساسة ومكوناتها التقنية، وجميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) ومكوناتها التقنية، ومنها: البنية التحتية، والمواقع الإلكترونية، وتطبيقات الويب، وتطبيقات الهواتف الذكية واللوحية، والبريد الإلكتروني والدخول عن بعد في <اسم الجهة>، وتنطبق هذه السياسة على جميع العاملين في <اسم الجهة>.

بنود السياسة

1- المتطلبات العامة

1-1 يجب على <اسم الجهة> إجراء اختبار الاختراق (Penetration Testing) دورياً، لتقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني.

2-1 تحدد <الإدارة المعنية بالأمن السيبراني> الأنظمة والخدمات والمكونات التقنية التي يجب إجراء اختبار الاختراق عليها وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

3-1 يجب على <اسم الجهة> إجراء اختبار الاختراق على جميع الخدمات المقدمة خارجياً ومكوناتها التقنية دورياً. (ECC-2-11-3-1)

4-1 يجب التأكد من أن اختبار الاختراق لا يؤثر على الأنظمة والخدمات المقدمة في <اسم الجهة>.

5-1 يجب على <اسم الجهة> إجراء اختبار الاختراق على الأنظمة الحساسة ومكوناتها التقنية كل ستة أشهر؛ على الأقل. (CSCC-2-10-2)

6-1 يجب إجراء اختبار الاختراق لاكتشاف نقاط الضعف الأمنية بكافة صورها والتي تشمل نقاط الضعف التي تنتج عادةً عن أخطاء في تطوير التطبيقات (Application Development Error) وضبط إعدادات النظام بشكل غير آمن (Configurations Faults) وإمكانية استغلال ثغرة محددة (Exploitability of Identified Vulnerability).

7-1 يجب تطوير إجراءات خاصة باختبار الاختراق واعتمادها ونشرها، مع الأخذ بالاعتبار عدم تأثيرها على سير الأعمال الخاصة بـ<اسم الجهة>.

اختر التصنيف

8-1 يجب على <الإدارة المعنية بالأمن السيبراني> تحديد أو الموافقة على أساليب اختبار الاختراق والأدوات والتقنيات التي يستخدمها فريق اختبار الاختراق الداخلي أو الخارجي قبل بدء عملية اختبار الاختراق.

9-1 في حال تفويض طرف خارجي للقيام باختبار الاختراق نيابة عن <اسم الجهة>، يجب التحقق من تطبيق جميع متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية ووفقاً لسياسة الأمن السيبراني المتعلّق بالأطراف الخارجية المعتمدة في <اسم الجهة>.

10-1 يجب تصنيف نتائج اختبار الاختراق بناءً على خطورتها، ومعالجتها حسب المخاطر السيبرانية المترتبة عليها ووفقاً لمنهجية إدارة المخاطر المعتمدة لدى <اسم الجهة>.

11-1 يجب وضع خطة عمل لمعالجة نتائج اختبار الاختراق يوضح فيها تأثير المخاطر وآلية معالجتها والمسؤول عن تطبيقها والفترة الزمنية اللازمة لتنفيذها.

2- متطلبات أخرى

1-2 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لعمليات اختبار الاختراق.

2-2 يجب مراجعة تطبيق متطلبات الأمن السيبراني لعمليات اختبار الاختراق في <اسم الجهة> دورياً. (ECC-2-11-4)

3-2 يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

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

2- **مراجعة السياسة وتحديثها:** <الإدارة المعنية بالأمن السيبراني>.

3- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بتقنية المعلومات> و<الإدارة المعنية بالأمن السيبراني>.

الالتزام بالسياسة

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

2- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذه السياسة.

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