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

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 <١,٠>

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

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المتعلقة بتقييم 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 في <اسم الجهة>. هذه المتطلبات تمت موائمتها مع متطلبات 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 العمل

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

بنود السياسة

١- البنود العامة

١-١ يجب صياغة وثيقة قواعد التنفيذ قبل بدء عملية اختبار الاختراق (Penetration Testing) والتي تغطي نطاق الاختبار، الصلاحيات، مدة الاختبار، الأنظمة المستهدفة، آلية الاختبار، الشروط والمتطلبات العامة وغيرها.

١-٢ يجب أن يشمل نطاق اختبار الاختراق جميع المكونات التقنية، ومنها: البنية التحتية، المواقع الإلكترونية، تطبيقات الويب، تطبيقات الهواتف الذكية واللوحية، البريد الإلكتروني والدخول عن بعد، وبيئة شبكات أنظمة التحكم الصناعي والشبكات المرتبطة بالشبكة التشغيلية لأنظمة التحكم الصناعي وذلك وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣ يجب إجراء اختبار الاختراق لتقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني دورياً.

١-٤ يجب إجراء اختبار الاختراق على الأنظمة الحساسة ومكوناتها التقنية وجميع خدماتها الداخلية والخارجية كل ستة أشهر على الأقل.

١-٥ يجب إجراء اختبار الاختراق على أنظمة العمل عن بعد وجميع الخدمات المقدمة خارجيًا (عن طريق الإنترنت) ومكوناتها التقنية مرة واحدة كل سنة على الأقل.

١-٦ يجب التأكد من أن تأثير الاختبار محدود على بيئة الإنتاج (البيئة قيد التشغيل) أو إجراء اختبار الاختراق في بيئة منفصلة مماثلة.

١-٧ يجب إجراء الاختبارات غير الفعالة (Passive Testing) لمراجعة وفحص الأنظمة والتطبيقات والشبكات والسياسات والإجراءات واكتشاف الثغرات الأمنية.

١-٨ يجب تطوير واعتماد خطة لاختبار الاختراق يوضح فيها نطاق العمل، تاريخ البدء والانتهاء، وآلية وسيناريوهات تنفيذ عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية.

١-٩ يجب التأكد من أن اختبار الاختراق لا يؤثر على الأنظمة والخدمات المقدمة في <اسم الجهة>.

١-١٠ يجب تعيين فريق مؤهل لديه الشهادات والخبرات ذات الصلة لضمان إجراء عمليات اختبار الاختراق بشكل فعّال.

١-١١ يجب على فريق اختبار الاختراق التنسيق مع الأطراف المعنية من داخل <اسم الجهة>، اتباع خطة إجراءات وخطة اختبار الاختراق المعتمدة، إجراء التحليلات اللازمة لتحديد المؤشرات الإيجابية الخاطئة، وتصنيف الثغرات وتحديد أسباب وجودها.

١-١٢ يجب معالجة البيانات التابعة لاختبار الاختراق بطريقة آمنة وجمعها وتخزينها ونقلها و إزالتها عندما تصبح غير ضرورية وفقًا لسياسة حماية البيانات والمعلومات المعتمدة لدى <اسم الجهة>.

١-١٣ يجب إجراء اختبار الاختراق لاكتشاف الثغرات الأمنية بكافة صورها والتي تشمل الثغرات التي تنتج عادةً عن أخطاء في تطوير التطبيقات (Application Development Error) دون الأخذ بعين الاعتبار معيار تطوير التطبيقات الآمن وضبط إعدادات النظام بشكل غير آمن (Misconfigurations) وإمكانية استغلال ثغرة محددة (Exploitability of Identified Vulnerability).

١-١٤ في حال تفويض طرف خارجي للقيام باختبار الاختراق نيابة عن <اسم الجهة>، يجب التحقق من تطبيق جميع متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية وفقًا لسياسة الأمن السيبراني المتعلّق بالأطراف الخارجية المعتمدة لدى <اسم الجهة>.

١-١٥ يجب إعداد تقرير لعرض نتائج الاختبار وتقديم التوصيات بعد إنتهاء عملية اختبار الاختراق.

١-١٦ يجب تصنيف نتائج اختبار الاختراق بناءً على خطورتها، ومعالجتها حسب المخاطر السيبرانية المترتبة عليها وفقًا لمنهجية إدارة المخاطر المعتمدة لدى <اسم الجهة>.

١-١٧ يجب وضع خطة عمل لمعالجة نتائج اختبار الاختراق يوضح فيها تأثير المخاطر وآلية معالجتها والمسؤول عن تطبيقها والفترة الزمنية اللازمة لتنفيذها ومتابعتها.

١-١٨ يجب إدارة حسابات المستخدمين المستخدمة لإجراء اختبار الاختراق ومراقبتها للتأكد من أنها تستخدم فقط لأغراض مشروعة، وإزالتها بعد انتهاء الاختبار.

١-١٩ يجب تطوير إجراءات ومعايير خاصة باختبار الاختراق بناء على حاجة العمل.

١-٢٠ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات عمليات اختبار الاختراق.

الأدوار والمسؤوليات

١- **مالك السياسة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

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

٣- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بتقنية المعلومات>.

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

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة السياسة سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالسياسة

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذه السياسة دوريًا.

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

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

اختر التصنيف

الإصدار <١,٠>