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 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.

اعتماد الوثيقة

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| التوقيع | التاريخ | الاسم | المسمى الوظيفي | الدور |
| <أدخل التوقيع> | اضغط هنا لإضافة تاريخ | <أدخل الاسم الكامل للموظف> | <أدخل المسمى الوظيفي> | اختر الدور |
|  |  |  |  |  |

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 |
|  |  |  |

قائمة المحتويات

[الغرض 4](#_Toc129611431)

[النطاق 4](#_Toc129611432)

[المعايير 4](#_Toc129611433)

[الأدوار والمسؤوليات 7](#_Toc129611434)

[التحديث والمراجعة 7](#_Toc129611435)

[الالتزام بالمعيار 7](#_Toc129611436)

# [الغرض](#_الأهداف" \o "يهدف هذا القسم إلى توضيح أسباب تطوير واعتماد المعيار وأهمية الالتزام بالمتطلبات المذكورة. كما يوضح هذا القسم علاقة المعيار بمتطلبات الضوابط الأساسية الصادرة من الهيئة الوطنية للأمن السيبراني ومتطلبات الأعمال والمتطلبات التنظيمية والتشريعية)

يهدف هذا المعيار إلى تحديد متطلبات الأمن السيبراني التفصيلية 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 اختراق الأصول التقنية في <اسم الجهة>. هذه المتطلبات تمت موائمتها مع سياسة اختبار الاختراق ومتطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني ويشمل ذلك على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018)، ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – 1: 2019) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

# النطاق

يطبق هذا المعيار على جميع أنظمة <اسم الجهة> الحساسة ومكوناتها التقنية، وجميع الخدمات المقدمة خارجيًا (عن طريق الإنترنت (ومكوناتها التقنية والتي تشمل البنية التحتية، والمواقع الإلكترونية، وتطبيقات الويب، وتطبيقات الهواتف الذكية واللوحية، والبريد الإلكتروني، والدخول عن بعد، وبيئة شبكات أنظمة التحكم الصناعي والشبكات المرتبطة بالشبكة التشغيلية، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

# [المعايير](#_الضوابط)

|  |  |
| --- | --- |
| 1 | المتطلبات العامة |
| الهدف | تحديد المتطلبات العامة والنطاق 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 | |
|  | يجب تطوير واعتماد خطة لاختبار الاختراق يوضح فيها نطاق العمل للتطبيقات والأنظمة وتاريخ البدء والانتهاء وآلية وسيناريوهات تنفيذ عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية. |
|  | يجب التأكد من أن خطة العمل لاختبار الاختراق متوافقة مع المتطلبات التشريعية والتنظيمية ذات العلاقة. |
|  | يجب التأكد من أن اختبار الاختراق يسير وفقًا لمنهجية محددة ومعتمدة ووفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة. |
|  | يجب صياغة وثيقة قواعد التنفيذ قبل بدء عملية اختبار الاختراق (Penetration Testing) وتتضمن هذه الوثيقة مالك النظام، مسؤول النظام، ضوابط الاتصال الرئيسية خلال الاختبار، الصلاحيات المعطاة لمسؤول الاختبار، نطاق الاختبار، الأجهزة النشطة والمنافذ والخدمات التابعة لها، نوع الاختبار، مدة الاختبار، عدد أعضاء فريق الاختبار، آلية اختبار الاختراق والأدوات والتقنيات المستخدمة التي يجب أن يتبعها فريق اختبار الاختراق الداخلي أو الخارجي، المتطلبات العامة وغيرها. |
|  | يجب إعداد تقرير لنتائج مفصلة لاختبار الاختراق يتضمن لأقسام التالية على الأقل:   * الملخص التنفيذي * مقدمة لإعداد التقارير * الأصول المستهدفة * المنهجية المتبعة في تصنيف الثغرات * مسار الهجوم * الجدول الزمني لأعمال التقييم * الاختبارات التي تم إجراؤها * التحديات * تفاصيل الملاحظات المكتشفة والتوصيات |
|  | بعد الانتهاء من تقرير اختبار الاختراق، 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. |
|  | يجب التأكد من أن تقنيات المستخدمين وأدواتهم وحساباتهم، وكذلك الأجهزة المستخدمة في اختبار الاختراق أو كانت جزءًا منه، خاضعة للتحكم والمراقبة وذلك لضمان استخدامها لغرض اختبار الاختراق فقط. |
|  | إزالة أو/و استعادة الأوضاع الطبيعية للتقنيات والأدوات وحسابات المستخدمين وكذلك الأجهزة المستخدمة في اختبار الاختراق أو كانت جزءًا منه، بعد الانتهاء من عملية اختبار الاختراق. |
|  | يجب إعداد تقرير لكل اختبار اختراق غير ناجح أو غير مكتمل توضح فيه تحديات التي واجهت فريق الاختبار لدراسة العوائق وحلها وإعادة الاختبار مرة أخرى. |
| 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 | |
|  | يجب إجراء اختبار الاختراق دوريًا وفقًا لسياسة اختبار الاختراق المعتمدة لدى <اسم الجهة>. |
|  | يجب إجراء اختبار الاختراق لجميع الخدمات المقدمة خارجيًا ومكوناتها التقنية دوريًا وحسب جدول محدد ووفقًا لمنهجية وإجراءات محددة ومعتمدة. |
|  | يجب إجراء اختبار الاختراق لجميع المكونات التقنية للأنظمة الحساسة، وجميع الخدمات المقدمة داخلياً وخارجياً بانتظام وبحسب جدول محدد (كل 6 أشهر) وفقًا لمنهجية وإجراءات محددة ومعتمدة. |
|  | يجب إجراء اختبار الاختراق لأنظمة العمل عن بعد مرة واحدة كل سنة على الأقل وفقًا لمنهجية وإجراءات محددة ومعتمدة. |
|  | يجب التأكد من تنفيذ اختبار الاختراق وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة، مع الأخذ بالاعتبار الإرشادات التالية:   * + 1. توفير المتطلبات الخاصة ببدء اختبار الاختراق الواردة في إجراءات اختبار الاختراق.     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.     3. 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).     4. تحديد الأنظمة أو الخدمات أو المكونات التقنية المستهدفة بالاختبار وأي معلومات أو صلاحيات يجب توفيرها قبل بدء اختبار الاختراق.     5. إجراء تقييمات غير مباشرة (Passive Assessment) لمراجعة وفحص الأنظمة والتطبيقات والشبكات والسياسات والإجراءات واكتشاف الثغرات الأمنية من خلال مراجعة الوثائق (Documentation Review)، مراجعة السجلات (Log Review)، مراجعة القواعد (Ruleset Review)، مراجعة إعدادات الأنظمة (System Configuration Review)، التنصت الشبكي على المعلومات (Network Sniffing)، أو فحص سلامة الملفات (File Integrity Checking).     6. يجب أن يتضمن اختبار الاختراق إنشاء منصة أو بيئة تحاكي الأنظمة أو الخدمات المستهدفة باختبار الاختراق لعمل الاختبار عليها بدلًا من الأنظمة والخدمات الإنتاجية الفعلية وتشمل بحد أدنى ما يلي:   + الهندسة الاجتماعية.   + اختبار الاختراق على مستوى الشبكة.   + اختبار الاختراق على مستوى التطبيق.   + اختبار الاختراق للشبكة اللاسلكية.     1. توثيق النتائج لكل خطوة من خطوات اختبار الاختراق. |

# [الأدوار والمسؤوليات](#_الأدوار_والمسؤوليات" \o "يهدف هذا القسم إلى تحديد الأدوار والمسؤوليات ذات العلاقة بهذا المعيار)

1. **مالك المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.
2. **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.
3. **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات>.
4. **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](#_الالتزام_بالسياسة" \o "يهدف هذا القسم إلى تحديد متطلبات الالتزام بالمعيار والنتائج المترتبة على مخالفتها أو انتهاكها)

1. يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دوريًا.
2. يجب على جميع 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>.