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 أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة

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 <1.0>

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	عُدِلَ 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 <1.0>

قائمة المحتويات

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بأجهزة المستخدمين ذات الصلاحيات الهامة والحساسة في <اسم الجهة>.

تمت مواءمة هذه المتطلبات مع متطلبات الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني وتشمل على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – 1: 2019) وضوابط الأمن السيبراني للحوسبة السحابية (CCC-1:2020) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل

يغطي هذا المعيار جميع الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة> وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

1	ضوابط أمن اجهزة المستخدمين (Workstation Security Controls)
الهدف	ضمان النشر الناجح لأجهزة المستخدمين الآمنة
المخاطر المحتملة	إذا لم يتم تطبيق تدابير الحماية بشكل صحيح على أجهزة المستخدمين، فسيترتب على ذلك مخاطر عالية قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها
الإجراءات المطلوبة	
1-1	عزل أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة بشكل منطقي ومادي على جزء مُخصص وآمن وموثوق من الشبكة.
2-1	تغطية أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة (PAWs) بنظام إدارة الصلاحيات الهامة والحسّاسة (PAM)، مع مراقبتها بشكل إضافي مقارنة بأجهزة المستخدمين الاعتيادية. كما يجب مراقبة وتسجيل جميع الأحداث الهامة والحساسة على أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة
3-1	أن تقوم <اسم الجهة> بتطبيق خدمات إدارة النقطة النهائية والتي تستخدم لأغراض مراقبة وضبط أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة بشكل ملائم.

4-1	ألا يتم استخدام البرمجيات العالية المخاطر في أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة إلا عند الضرورة للعمل، على ألا تكون الأجهزة متصلة بالإنترنت.
5-1	أن تتضمن أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة سياسة السماح بقائمة محددة من التطبيقات لاستخدام تطبيقات البرمجيات أو الملفات القابلة للتنفيذ التي تم التحقق منها واعتمادها فقط لتقديم خدمات مخصصة.
6-1	ألا تكون أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة متصلة بالشبكات اللاسلكية.
7-1	تطبيق حزم التحديثات والإصلاحات الأمنية على برمجيات أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة حال توافرها ووفقًا لإجراءات إدارة التغيير المعمول بها في <اسم الجهة>. ويجب ألا تتسبب عملية التحديثات والإصلاحات الأمنية في انقطاع عمل أي تطبيقات ضرورية لإدارة الصلاحيات والامتيازات الهامة والحساسة.
8-1	أن يقتصر الوصول إلى أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة على مديرين محددين للنظام من خلال السماح بالوصول فقط باستخدام قوائم التحكم بالوصول (ACL) إلى حسابات المديرين، والتي يجب فصلها عن حساباتهم العادية واستخدامها فقط لغرض معين.
9-1	تعطيل أو تغيير اسم الحسابات الافتراضية/غير التفاعلية/غير الضرورية
10-1	ضبط إعدادات وقت انتهاء الجلسة وإغلاق الجلسة في حال عدم الاستخدام وفقًا لسياسات الأمن السيبراني المطبقة في <اسم الجهة>.
11-1	ضبط إعدادات كلمات المرور لمُحمِّل تشغيل (Bootloader) نظام الإدخال/الإخراج الأساسي (BIOS)على جميع أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة.
12-1	تطبيق نظام منع الاختراقات في المستضيف (HIPS) على جميع أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة لمنع الهجمات المعروفة وغير المعروفة

13-1	نشر جدار حماية من البرمجيات المستضافة على جميع أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة للتحكم في سلوك تطبيقات النظام الفردية على شبكة معينة.
14-1	نشر البرمجيات المضادة للفيروسات وتقنية كشف نقطة النهاية والاستجابة لها على جميع أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة.
15-1	نشر أنظمة منع تسّرب البيانات على جميع أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة.
2	الأجهزة التي تتمتع بصلاحيات ومزايا (Hardware root of trust)
الهدف	التأكد من إجراء عملية تحصين مناسبة لأجهزة المستخدمين من خلال إيجاد "جذور الثقة root of trust". ويجب اختيار التقنيات المناسبة لتحقيق هذا الهدف.
المخاطر المحتملة	قد تؤدي عملية التحصين غير السليمة إلى وجود ثغرات في الأجهزة ومتجهات الهجمات، وقد يترتب على ذلك مخاطر عالية قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-2	أن تكون أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة قائمة على أجهزة موثوقة مقدمة من مورّد أو طرف خارجي موثوق ومعتمد. ويجب صيانة الأجهزة من قبل مورّد موثوق بشكل دوري.
2-2	تسجيل ومراقبة أي تغييرات على أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة (خاصة فيما يتعلق بنظام التشغيل). ويجب ضبط إعدادات حلول السجل بحيث تقتصر على إرسال السجلات المحددة فقط إلى نظام السجلات المركزي، مثل: استخدام بروتوكول SYSLOG وصيغ السجلات CEF أو LEEF أو RFC 5425 specified log format.
3-2	أن تقوم أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة بتنفيذ إجراء تشغيل آمن لضمان استخدام أجهزة المستخدمين للبرامج التي تثق بها الجهة المصنعة للمعدات الأصلية.

4-2	تحديث برامج تشغيل أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة، باستخدام أفضل ممارسات الأمن السيبراني (مثل: مقارنة دوال التجزئة).
5-2	أن تدعم أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة (PAWs) تقنية سلامة الشفرة المحمية بمراقب الأجهزة الافتراضية (HVCI) لعزل دالة اتخاذ القرارات المتعلقة بسلامة الشيفرة عن بقية نظام التشغيل (نظام ويندوز فقط).
6-2	أن تقوم أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة بنشر حماية الوصول إلى الذاكرة المباشرة (DMA) في النواة لمنع هجمات الوصول إلى الذاكرة من الأجهزة الخارجية الخبيثة.
7-2	أن تقوم أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة بنشر تدابير أمن البرمجيات لحماية وسلامة النظام.
8-2	في حالة بدء التشغيل، يجب أن تتحقق أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة من الحفاظ على سلامة النظام من خلال المصادقة المحلية أو عن بُعد.
3	معايير أخرى (Other Standard Controls)
الهدف	تطبيق جميع المعايير والمتطلبات الإلزامية المعمول بها على أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة لضمان أعلى مستويات الحماية.
المخاطر المحتملة	قد يؤدي الإخفاق في المواءمة مع المعايير والمتطلبات الأمنية الخاصة ب<اسم الجهة> إلى سرقة المعلومات والكشف عنها والوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-3	تطبيق المعايير التالية فيما يتعلق بأجهزة المستخدمين ذات الصلاحيات الهامة والحساسة: 1. أمن الأنظمة الافتراضية 2. إدارة المفاتيح 3. جهة إصدار الشهادات 4. التشفير

	5. تسجيل الأحداث وسجلات التدقيق 6. الأمن المادي 7. الإعدادات والتحصين الآمن

الأدوار والمسؤوليات

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 عند 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

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

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>.