هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. والبنود الملونة باللون الأخضر هي أمثلة يجب حذفها. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج معيار الإعدادات والتحصين الآمن

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.

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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	عُدِّلَ 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

اختر التصنيف

الإصدار <1.0>

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بمتطلبات الإعدادات والتحصين الآمن للأنظمة الخاصة ب<اسم الجهة> وذلك لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية.

تمت موائمة هذا المعيار مع الضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

يطبق هذا المعيار على جميع الأنظمة التقنية الخاصة ب<اسم الجهة>، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

1	تحديد المعايير الأمنية الأساسية (Security baseline standards (definition
الهدف	تحديد المعايير الأمنية الأساسية (بما في ذلك الإعدادات الأساسية) للبنية التحتية للأنظمة.
المخاطر المحتملة	قد يؤدي عدم وجود معايير الإعدادات إلى حذف الإعدادات والإعدادات الأمنية المطلوبة، وقد يؤدي ذلك إلى دقة الأنظمة أو البنية التحتية ذات الثغرات والمشاكل النشطة وزيادة الصيانة والترقية بسبب عدد الإصدارات المنتشرة.
الإجراءات المطلوبة	
1-1	تحديد وتوثيق واعتماد المعايير الأمنية الأساسية ومقاييس الإعدادات للبنية التحتية للأنظمة.
2-1	إعداد المعايير الأمنية الأساسية لما يلي: أ) أجهزة المستخدم النهائي بما في ذلك الأجهزة اللوحية والهواتف المحمولة ب) أجهزة الشبكة بما في ذلك جدران الحماية والموجهات والمبدلات ج) أنظمة تشغيل الشبكة د) الخوادم ه) أنظمة التشغيل و) تطبيقات الأعمال (بما في ذلك تطبيقات وسائل التواصل الاجتماعي)

	ز) البنية التحتية للوصول عن بُعد والعمل عن بُعد، بما في ذلك الخوادم والشبكة الافتراضية الخاصة وأجهزة المستخدم النهائي ح) الأنظمة الحساسة الأخرى التي حددتها الإدارة
3-1	يجب أن تشير القواعد الأساسية الأمنية إلى ما يلي: أ) الإرشادات أو التعليمات المنشورة من قبل الجهة المصنعة ب) التحديثات أو التصحيحات أو حزم التحديثات أو الإعدادات الصادرة عن الجهة المصنعة ج) تقييم مخاطر الأمن السيبراني الخاصة بـ <اسم الجهة> د) تقارير إدارة مسح الثغرات ه) نتائج الاختبارات الأمنية و) معلومات حول أفضل الممارسات الأمنية الموثوقة على المستوى العالمي وعلى المستوى الوطني ز) سياسات <اسم الجهة> التي تتطلب متطلبات معينة
4-1	تحديد وتطبيق المعايير الأساسية والإعدادات الآمنة الخاصة بـ <اسم الجهة> على التطبيقات والخدمات القائمة على الحوسبة السحابية والمستضافة كخدمة (البرمجيات كخدمة، المنصة كخدمة، البنية التحتية كخدمة)
5-1	تغيير كلمات المرور الافتراضية لجميع الحسابات وإنشاء كلمات مرور جديدة عند تسجيل الدخول لأول مرة. وإنشاء كلمات مرور جديدة وفقًا لسياسة ومعيار إدارة الهوية والوصول الخاصة بـ <اسم الجهة>.
6-1	إعداد البرمجيات لتعطيل الخدمات والوظائف غير المطلوبة للاستخدام من قبل عمليات <اسم الجهة>، في الحالات التي تشكل هذه الخدمات والوظائف خطرًا على <اسم الجهة>.
7-1	الاحتفاظ بسجل للخدمات والوظائف المعطلة من قبل <اسم الجهة> لاستخدامه في تهيئة الإعدادات والتكوينات.

8-1	أن تتضمن الإعدادات والمعايير الأساسية الآمنة تزامنًا مركزيًا للوقت مع مصدر دقيق وموثوق به، على سبيل المثال الهيئة السعودية للمواصفات والمقاييس والجودة.
9-1	بناء الإعدادات وفقاً للمعايير المبنية والصور وملفات الإعدادات القياسية التي تم إنشاؤها من بنية أنظمة رئيسية خاضعة للرقابة.
10-1	حفظ المعايير الأمنية الأساسية والإعدادات والصور والملفات بطريقة آمنة مع تقييد الوصول إليها من الأفراد المصرح لهم وباتباع ضوابط الوصول المادي والمنطقي.
11-1	حماية المعايير الأمنية والاساسية والإعدادات والصور والملفات من الوصول والتغيير والإفصاح غير المصرح بهم وذلك باتباع الضوابط المنطقية والمادية.
12-1	أن يقتصر الوصول إلى المعايير الأمنية الأساسية ووثائق الإعدادات الآمنة على الأفراد المناسبين داخل <اسم الجهة>.
2	تطبيق ونشر الإعدادات الآمنة (Secure configuration implementation (and deployment
الهدف	تنفيذ ونشر الإعدادات آمنة على مستوى الجهة.
المخاطر المحتملة	قد يؤدي عدم تطبيق الإعدادات القياسية إلى ترك الجهة بمزيج من الإعدادات والثغرات والمشاكل النشطة في بيئة الإنتاج، وزيادة الصيانة والنفقات العامة.
الإجراءات المطلوبة	
1-2	بناء جميع الأنظمة والأجهزة والبرمجيات الجديدة وإعدادها وفقًا للمعايير الأساسية والإعدادات الآمنة المعتمدة، باستخدام الوحدات والصور والملفات ذات الصلة.
2-2	اختبار جميع الأنظمة والأجهزة والبرمجيات الجديدة بنجاح قبل التنفيذ / إطلاق لضمان تلبيتها للمعايير الاساسية والإعدادات.

3-2	إيقاف تشغيل الأنظمة أو الأجهزة أو البرمجيات التي لا تلبي المعايير الأمنية المعتمدة.
4-2	نشر التطبيقات والخدمات المستندة إلى السحابة والمستضافة (بما في ذلك البرمجيات كخدمة / المنصة كخدمة/ البنية التحتية كخدمة) باتباع المعايير والاعدادات الاساسية للتطبيقات المستندة إلى السحابة والمستضافة المعتمدة لدى <اسم الجهة>.
5-2	تثبيت الإعدادات الاساسية الآمنة على الأنظمة الحالية في أقرب وقت ممكن خلال فترات الصيانة المتفق عليها.
6-2	معالجة الأنظمة أو الأجهزة أو البرمجيات التي لا تلبي المعايير والإعدادات الاساسية الأمنية المعتمدة من خلال تطبيق المعايير والإعدادات الامنية الاساسية المعتمدة في أسرع وقت عملي ممكن وخلال فترات الصيانة المتفق عليها.
3	تحديث الإعدادات الآمنة (Update secure configurations)
الهدف	ضمان تحديث الإعدادات الآمنة ومراجعتها بانتظام وتحديثها بطريقة خاضعة للرقابة.
المخاطر المحتملة	قد يؤدي استخدام الإعدادات غير المحدثة إلى تعريض الجهة للتهديدات الجديدة أو الحالية، وتقليل أداء الوظائف، وتقليل الأداء، ونشر الأنظمة أو البنية التحتية مع نقاط الضعف المعروفة والنشطة.
الإجراءات المطلوبة	
1-3	مراجعة المعايير الأمنية الأساسية والإعدادات الآمنة مرة واحدة سنويًا على الأقل أو بعد أي تغيير مهم في البنية التحتية أو الأجهزة أو البرامج في <اسم الجهة>.
2-3	مراجعة الأنظمة والأجهزة والبرامج التي تم نشرها مرة واحدة على الأقل سنويًا لضمان نشر المعايير والإعدادات الآمنة المعتمدة.
3-3	اتباع إجراءات إدارة التغيير لتحديث للمعايير الأمنية والإعدادات الأساسية.

4-3	تقييم التطبيقات والخدمات السحابية والمستضافة مرة واحدة سنويًا على الأقل لضمان نشر التطبيقات والخدمات باستخدام المعايير الأساسية والإعدادات المعتمدة.
5-3	تحديث المعايير الأساسية والإعدادات الآمنة المستخدمة إلى النسخة المعتمدة في أقرب وقت ممكن وخلال فترات الصيانة المتفق عليها.
6-3	تقييم البنية التحتية وأنظمة العمل عن بُعد مرة واحدة سنويًا على الأقل لضمان توفير الوصول عن بُعد باستخدام المعايير الأساسية والإعدادات الآمنة المعتمدة.
4	إعداد برمجيات مكافحة البرامج الضارة (Anti-malware software configuration)
الهدف	حماية أصول تقنية المعلومات المستخدمة لدى <اسم الجهة> من البرمجيات الضارة.
المخاطر المحتملة	قد يؤدي عدم وجود برامج مكافحة البرامج الضارة إلى تعريض أصول تقنية المعلومات في الجهة للإصابة والهجوم بسبب البرمجيات الخبيثة، مما يؤدي إلى فقدان أو تلف البيانات والمعلومات وانخفاض الإنتاجية وزيادة معدل الخطأ والإغلاق غير المتوقع.
الإجراءات المطلوبة	
1-4	تثبيت برنامج مكافحة البرامج الضارة المعتمد لدى <اسم الجهة> على جميع الخوادم والعملاء (أي أنظمة سطح المكتب، والحاسوب المحمول، والأجهزة اللوحية، والهواتف الجوالة).
2-4	يجب، كحد أدنى، إعداد مكافحة البرامج الضارة بالقدرات التالية: أ) الكشف عن البرمجيات الضارة المعتمدة و/أو غير الموقعة ب) إعداد التنبيهات لتسجيل الدخول والمراقبة.
3-4	يجب إعداد برنامج مكافحة البرامج الضارة كحد أدنى من أجل تحقيق ما يلي: أ) الاتصال بالشبكة تلقائيًا ب) التشغيل المستمر و/أو إجراء مسح منتظم للبرمجيات الضارة ج) التحقق من التحديثات وتنزيلها تلقائيًا بالوتيرة المحددة

	د) تسجيل جميع الأنشطة التي يقوم بها البرنامج ه) إصدار تنبيهات إلى المسؤول عن المستخدم وإرسال تنبيهات إلى نظام المراقبة المركزي (مثل: مركز العمليات الأمنية) و) طلب وصول مميز لإجراء تغييرات على التشغيل.
4-4	تثبيت أنظمة منع التسلل القائمة على المضيف وأنظمة كشف التسلل القائمة على المضيف على جميع الخوادم المستخدمة وأجهزة الحاسوب المكتبية والمحمولة والأجهزة اللوحية الخاصة بـ <اسم الجهة> (حيث يكون النظام قادرًا على تشغيل نظام منع التسلل إلى الأجهزة المضيفة ونظام منع التطفل المستند إلى المضيف)
5-4	يجب، كحد أدنى، إعداد نظام منع التسلل إلى الأجهزة المضيفة من أجل: أ) الاتصال بالشبكة تلقائيًا ب) العمل بشكل مستمر ج) التحقق من التحديثات وتنزيلها تلقائيًا بالوتيرة المحددة د) تسجيل جميع التنبيهات والأنشطة المحظورة وحركة المرور التي تتم معالجتها من قبل نظام منع التسلل إلى الأجهزة المضيفة ه) إصدار تنبيهات للمستخدم وإلى نظام مراقبة مركزي (مثل: مركز العمليات الأمنية) و) طلب وصول مميز لإجراء تغييرات على التشغيل.
6-4	يجب تهيئة الأصول المقدمة بموجب اتفاقيات الأطراف الخارجية لتلبية متطلبات هذا المعيار.
7-4	يجب تحديد وتسجيل ومراجعة أصول الأطراف الخارجية التي لا تلبي متطلبات هذا المعيار.
8-4	يجب إعداد أنظمة بوابات البريد الإلكتروني للحماية من البرامج الضارة وفقًا لسياسة ومعيار حماية البريد الإلكتروني الخاص ب <اسم الجهة>.

5	إعدادات الأنظمة الحساسة (Critical systems configuration)
الهدف	تطبيق ضوابط إضافية لإعدادات آمنة على الأنظمة الحساسة.
المخاطر المحتملة	قد لا توفر الإعدادات والتكوينات وعمليات الضبط القياسية مستوى الحماية المطلوب للأنظمة الحساسة، وبالتالي قد تخضع هذه الأنظمة لمستويات أعلى من التهديدات وارتفاع وتيرة الهجمات وارتفاع مستويات التأثير على الأعمال في حال تعطل تشغيل النظام.
الإجراءات المطلوبة	
1-5	مراجعة المعايير الأمنية الأساسية والإعدادات الآمنة للأنظمة الحساسة كل ستة أشهر على الأقل أو بعد أي تغيير كبير في البنية التحتية أو الأجهزة أو البرمجيات، بالإضافة إلى أي تغييرات في المتطلبات القانونية والتنظيمية ذات الصلة.
2-5	مراجعة الأنظمة والأجهزة والبرمجيات الحساسة المستخدمة كل ستة أشهر على الأقل لضمان تطبيق المعايير الأساسية والإعدادات الآمنة المعتمدة.
3-5	تحديث المعايير الأساسية والإعدادات الآمنة المستخدمة إلى النسخة المعتمدة في أقرب وقت ممكن وخلال فترات الصيانة المتفق عليها.

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 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.

اختر التصنيف

الإصدار <1.0>

الالتزام بالمعيار

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>.