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 الإعدادات والتحصين

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 "<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

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

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بحماية وتحصين وضبط إعدادات الأصول المعلوماتية والتقنية والتطبيقات الخاصة ب<اسم الجهة> للحد من المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية في <اسم الجهة> للمحافظة على سرية المعلومات، وسلامتها، وتوافرها.

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

نطاق العمل

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية والتطبيقات الخاصة ب<اسم الجهة>، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

1- البنود العامة

1-1 يجب تحديد وتوثيق جميع الأصول المعلوماتية والتقنية المستخدمة داخل <اسم الجهة> وكذلك التطبيقات والبرمجيات المعتمدة.

2-1 يجب تحصين وضبط إعدادات أجهزة الحاسب الآلي، والأنظمة، والتطبيقات، وأجهزة الشبكات، والخوادم والأجهزة الأمنية الخاصة ب<اسم الجهة> بما يتوافق مع المعايير التقنية الأمنية المعتمدة من قبل المورد وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات الدولية لتصدي الهجمات السيبرانية.

3-1 يجب تعطيل خاصية التصوير (Print Screen or Screen Capture) للأجهزة التي تنشئ أو تعالج المعلومات بناءً على تصنيف تلك المعلومات.

4-1 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية أمن الإعدادات والتحصين.

2- تطوير المعايير الأمنية التقنية:

1-2 يجب استخدام دليل الإعدادات والتحصين (Security Configuration Guidance) الخاص بالمُورد وذلك وفقًا للسياسات والإجراءات التنظيمية الخاصة ب<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات الدولية.

2-2 يجب استخدام دليل الإعدادات والتحصين من مصادر موثوقة ومتوافقة مع المعايير المصنعية، مثل: مركز أمن الإنترنت (CIS)، ومعهد الأمن والشبكات وإدارة النظم (SANS)، والمعهد الوطني للمعايير والتقنية (NIST).

3-2 يجب تطوير معايير أمنية تقنية خاصة ب<اسم الجهة> بما يتناسب مع طبيعة الأعمال وبما يتوافق مع دليل الإعدادات والتحصين الخاص بالمورد والمعايير المصنعية ووفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

4-2 يجب تطوير وتوثيق واعتماد ومراجعة المعايير التقنية الأمنية (Technical Security Standards) الخاصة بجميع الأصول المعلوماتية والتقنية والتطبيقات والبرمجيات المصرح باستخدامها لدى <اسم الجهة>، وفقًا لأفضل الممارسات الدولية والسياسات والإجراءات التنظيمية المعتمدة لدى <اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

3- مراجعة الإعدادات والتحصين والتأكد من تطبيقها في الحالات التالية:

1-3 يجب مراجعة الإعدادات والتحصين لجميع الأنظمة للأصول المعلوماتية والتقنية والتطبيقات مرة واحدة كل سنة على الأقل أو عند وجود تغييرات، والتأكد من تطبيقها بما يتوافق مع إرشادات الأمن السيبراني، وأفضل الممارسات، والتوصيات الخاصة بالموردين (Vendors)، وبما يتوافق مع آليات إدارة التغيير المتبعة في <اسم الجهة>.

2-3 يجب مراجعة الإعدادات والتحصين قبل إطلاق وتدشين التطبيقات والمشاريع التقنية والتغييرات المتعلقة بالأصول المعلوماتية والتقنية.

3-3 يجب مراجعة وتحصين الإعدادات المصنعية (Default Configuration) لجميع الأصول التقنية وللأصول التقنية لأنظمة العمل عن بعد، ومنها التأكد من عدم وجود كلمات مرور ثابتة، وخلفية افتراضية.

4-3 يجب تقييد تفعيل الخصائص والخدمات في أنظمة العمل عن بعد حسب الحاجة على أن يتم تقييم المخاطر السيبرانية المحتملة في حال الحاجة لتفعيلها وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

5-3 يجب اعتماد نسخة (Image) لإعدادات وتحصين الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة> وفقًا للمعايير التقنية الأمنية المعتمدة، وحفظها في مكان آمن.

6-3 يجب استخدام نسخة (Image) معتمدة في تثبيت أو تحديث الأصول المعلوماتية والتقنية.

7-3 يجب توفير التقنيات اللازمة لإدارة الإعدادات والتحصين مركزيًا، والتأكد من إمكانية تطبيق أو تحديث الإعدادات والتحصين تلقائيًا لكافة الأصول المعلوماتية والتقنية في مواعيد زمنية محددة ومخطط لها، بعد إجراء الاختبارات اللازمة.

8-3 يجب توفير نظام مراقبة الإعدادات المتوافقة مع بروتوكول أتمتة المحتوى الأمني (Security Content Automation Protocol "SCAP") للتأكد من أن الإعدادات متوافقة مع المعايير التقنية الأمنية المعتمدة ومطبقة بشكل كامل، كما يجب الإبلاغ عن أي تغييرات غير مصرّح بها.

9-3 مزامنة التوقيت (Clock Synchronization) مركزيًا ومن مصدر دقيق وموثوق (مثل ما توفره الهيئة السعودية للمواصفات والمقاييس والجودة من مصادر ذات علاقة).

الأدوار والمسؤوليات

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

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

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

4- **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

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

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>.