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

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة.
وللقيام بذلك، اتبع الخطوات التالية:

1. اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
2. أضف "<الجهة>" في مربع البحث عن النص.
3. أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
4. اضغط على "المزيد" وتأكّد من اختيار "Match case".
5. اضغط على "استبدل الكل".
6. أغلق مربع الحوار.

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل الاسم الكامل للشخص>	اضغط هنا لإضافة نص	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

اختر التصنيف

الإصدار 1.0

قائمة المحتويات

الأهداف 3
نطاق العمل وقابلية التطبيق 3
بنود السياسة 3
الأدوار والمسؤوليات 4
الالتزام بالسياسة 5

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية وتحصين وضبط إعدادات الأصول المعلوماتية والتقنية والتطبيقات الخاصة بـ<اسم الجهة> لمقاومة الهجمات السيبرانية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٦-٢-٢ والضابط رقم ١-٦-٣-٥ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة عن الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية والتطبيقات الخاصة بـ<اسم الجهة>، وتنطبق على جميع العاملين في <اسم الجهة>.

بنود السياسة

1- يجب تحديد جميع الأصول المعلوماتية والتقنية المستخدمة داخل <اسم الجهة> وكذلك التطبيقات والبرمجيات المعتمدة والتأكد من توفير معايير تقنية أمنية (Technical Security Standards) لها.

2- يجب تطوير وتوثيق واعتماد المعايير التقنية الأمنية الخاصة بجميع الأصول المعلوماتية والتقنية والتطبيقات والبرمجيات المصرح بها داخل <اسم الجهة>.

3- يجب تحصين وضبط إعدادات أجهزة الحاسب الآلي، والأنظمة، والتطبيقات، وأجهزة الشبكات، والأجهزة الأمنية الخاصة بـ<اسم الجهة> بما يتوافق مع المعايير التقنية الأمنية المعتمدة لمقاومة الهجمات السيبرانية.

4- يجب استخدام إحدى الطرق التالية لتطوير المعايير الأمنية التقنية:

1-4 دليل الإعدادات والتحصين (Security Configuration Guidance) الخاص بالمُورد وذلك وفقاً للسياسات والإجراءات التنظيمية الخاصة بـ<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات الدولية.

2-4 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)، ووكالة أنظمة معلومات الدفاع (DISA)، ودليل التطبيق الفني الأمني (STIG)، وغيرها.

3-4 تطوير معايير أمنية تقنية خاصة بـ<اسم الجهة> بما يتناسب مع طبيعة الأعمال وبما يتوافق مع دليل الإعدادات والتحصين الخاص بالمورد والمعايير المصنعية.

5- يجب أن تغطي الضوابط الخاصة بالمعايير التقنية الأمنية بحد أدنى ما يلي:

1-5 إيقاف أو تغيير الحسابات المصنعية والافتراضية.

2-5 منع تثبيت البرمجيات غير المرغوب بها.

3-5 تعطيل منافذ الشبكة غير المستخدمة.

4-5 تعطيل الخدمات غير المستخدمة.

5-5 تقييد استخدام وسائط الحفظ والتخزين الخارجي.

6-5 تغيير الإعدادات الافتراضية التي قد تُستغل في الهجمات السيبرانية.

6- يجب مراجعة الإعدادات والتحصين والتأكد من تطبيقها في الحالات التالية:

1-6 مراجعة الإعدادات والتحصين للأصول المعلوماتية والتقنية والتطبيقات دورياً والتأكد من تطبيقها وفقاً للمعايير التقنية الأمنية المعتمدة.

2-6 مراجعة الإعدادات والتحصين قبل إطلاق وتدشين المشاريع والتغييرات المتعلقة بالأصول المعلوماتية والتقنية.

3-6 مراجعة الإعدادات والتحصين قبل إطلاق وتدشين التطبيقات.

4-6 مراجعة الإعدادات والتحصين لأنظمة التحكم الصناعي دورياً والتأكد من تطبيقها وفقاً للمعايير التقنية الأمنية المعتمدة.

7- يجب اعتماد صورة (Image) لإعدادات وتحصين الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> وفقاً للمعايير التقنية الأمنية، وحفظها في مكان آمن.

8- يجب استخدام صورة (Image) معتمدة في تثبيت أو تحديث الأصول المعلوماتية والتقنية.

9- يجب توفير التقنيات اللازمة لإدارة الإعدادات والتحصين مركزياً، والتأكد من إمكانية تطبيق أو تحديث الإعدادات والتحصين تلقائياً لكافة الأصول المعلوماتية والتقنية في مواعيد زمنية محددة ومخطط لها.

10- 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.

11- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة الإعدادات والتحصين.

12- يجب مراجعة متطلبات الأمن السيبراني المتعلقة بالإعدادات والتحصين للأصول المعلوماتية والتقنية والتطبيقات الخاصة بـ<اسم الجهة> سنوياً، أو في حالة حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

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

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

الالتزام بالسياسة

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذه السياسة دورياً.

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>.