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 إدارة سجلات الأحداث ومراقبة الأمن السيبراني

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 "<اسم 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>

قائمة المحتويات

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

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير؛ لتقليل المخاطر السيبرانية، وحماية الأصول المعلوماتية لـ<اسم الجهة> من التهديدات (Threats) الداخلية والخارجية، عن طريق استخدام نظام إدارة سجلات الأحداث، ومراقبة الأمن السيبراني.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة إدارة سجلات الأحداث، ومراقبة الأمن السيبراني الخاصة بـ<اسم الجهة>، وتنطبق على جميع العاملين في <اسم الجهة>.

بنود السياسة

1- البنود العامة

1-1 يجب توفير تقنيات إدارة المعلومات، والأحداث الأمنية (Security Information and Event Management "SIEM") اللازمة، لجمع سجلات الأحداث السيبرانية للأصول المعلوماتية، والأنظمة والتطبيقات، وقواعد البيانات والشبكات، وأنظمة الحماية في <اسم الجهة>. ويجب أن تحتوي هذه السجلات على المعلومات الآتية بوصفها حداً أدنى:

1-1-1 نوع الحدث (Event Type)
1-1-2 مكان الحدث، أو النظام الذي تم تنفيذ الحدث عليه (Location of Event or System)
1-1-3 وقت الحدث وتاريخه (Date and Time of Event)
1-1-4 المستخدم أو الأداة المستخدمة لتنفيذ الحدث
1-1-5 حالة الحدث أو نتيجته (Success vs. Failure)

2- الأحداث المراد تسجيلها

1-2 يجب أن تفعّل الأنظمة المراد مراقبتها سجلات الأحداث عند وقوع أحد الأحداث، بحد أدنى؛ ما يلي:

1-1-2 الأحداث (Event Logs) الخاصة بالأمن السيبراني على جميع المكونات التقنية للأنظمة الحساسة (أنظمة التشغيل، قواعد البيانات، التخزين، التطبيقات، والشبكات).

2-1-2 الأحداث (Event Logs) الخاصة بالأمن السيبراني للشبكة الصناعية والاتصالات المرتبطة بها.

3-1-2 الأحداث الخاصة بالحسابات التي تمتلك صلاحيات مهمة وحساسة على الأصول المعلوماتية.

4-1-2 الأحداث الخاصة بالتصفح والاتصال بالإنترنت، والشبكة اللاسلكية.

2-1-5 نقل المعلومات عبر وسائط التخزين الخارجية.

2-1-6 إجراء تغييرات غير مشروعة على السجلات، وملفات الأنظمة الحساسة من خلال تقنيات إدارة تغييرات الملفات ("FIM" File Integrity Management).

2-1-7 تغيير إعدادات النظام، أو الشبكة، أو الخدمات، بما في ذلك تنزيل حزم التحديثات والإصلاحات، أو غيرها من التغييرات على البرامج المثبتة.

2-1-8 أنشطة مشبوهة، مثل الأنشطة التي يكتشفها نظام منع التسلل (Intrusion Prevention System "IPS")

2-2 يجب إعداد إجراءات ومعايير أمنية تطبق أفضل الممارسات؛ لحفظ سجلات الأحداث بطريقة تضمن سلامتها من التعديل، أو الحذف، أو الوصول غير المصرح به.

2-3 يجب مراقبة سجلات الأحداث، وتحليلها دورياً حسب تصنيفها، بما في ذلك مراقبة سلوك مستخدم الأنظمة الحساسة وتحليله.

2-4 يجب مزامنة التوقيت (Clock Synchronization) مركزياً، ومن مصدر دقيق وموثوق، لجميع الأنظمة التي تتم مراقبتها.

2-5 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لنظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

2-6 يجب أرشفة سجلات الأحداث، والقيام بالنسخ الاحتياطي دورياً.

2-7 يجب أن تكون مدة الاحتفاظ بسجلات الأحداث السيبرانية 12 شهراً على الأقل، و18 شهراً بالنسبة للأنظمة الحساسة بحد أدنى، وبما يتوافق مع السياسات الداخلية، والمتطلبات التشريعية والتنظيمية 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> و <الإدارة المعنية بالأمن السيبراني>.

الالتزام بالسياسة

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

2- يجب على جميع العاملين في <اسم الجهة> الالتزام بهذه السياسة.

3- قد يُعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.