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

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	عُدِّل 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 <١,٠>

قائمة المحتويات

الغرض ٤
نطاق العمل ٤
بنود السياسة ٤
الأدوار والمسؤوليات ٦
التحديث والمراجعة ٦
الالتزام بالسياسة ٦

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بأنظمة إدارة سجلات الأحداث والمراقبة الخاصة ب<اسم الجهة> لتقليل المخاطر السيبرانية عليها وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: 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 أنظمة إدارة سجلات الأحداث، ومراقبة الأمن السيبراني الخاصة ب<اسم الجهة>، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>. كما يجب أن تتوافق هذه السياسة مع النموذج التشغيلي لمراكز عمليات الأمن السيبراني المدارة والمتطلبات التشريعية للهيئة الوطنية للأمن السيبراني.

بنود السياسة

١- **البنود العامة**

١-١ يجب توفير أنظمة مراقبة تتوافق مع مستوى المخاطر والمتطلبات التنظيمية للهيئة الوطنية للأمن السيبراني، بحيث تقوم بجمع وتحليل سجلات الاحداث السيبرانية للأصول المعلوماتية، والأنظمة والتطبيقات، وقواعد البيانات والشبكات، وأنظمة الحماية في <اسم الجهة>. ويجب أن تحتوي هذه السجلات على المعلومات الآتية بوصفها حدًا أدنى:

١-١-١ نوع الحدث (Event Type).

١-١-٢ مصدر الحدث (IIS, EDR, AV, Sys mon, security logs, etc…)

١-١-٣ النظام الذي تم تنفيذ الحدث منه (e.g. mail server)

١-١-٤ وقت الحدث وتاريخه (Date and Time of Event).

١-١-٥ المستخدم أو الأداة المستخدمة لتنفيذ الحدث.

١-١-٦ حالة الحدث أو نتيجته (Success vs. Failure).

١-٢ يجب تفعيل وجمع سجلات الأحداث (Event Logs) والتدقيق (Audit Trial) وعمليات الدخول (Login) لجميع الأصول التقنية ذات العلاقة وحسب سجل المخاطر ل<اسم الجهة> بما فيها الأنظمة التقنية السحابية (CTS) والأنظمة الحساسة والأنظمة التشغيلية وأنظمة العمل عن بعد والأصول التقنية الخاصة بحسابات التواصل الاجتماعي وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣ يجب حماية سجلات أحداث الأمن السيبراني من التغيير والإفشاء والتلف والوصول غير المصرح به والإصدار غير المصرح به، وحماية سجلات الأحداث لجميع الأنشطة بهدف دعم عمليات التحليل الرقمي الجنائي (Digital Forensics) في حال الحاجة لذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٤ يجب استخدام وسائل التحكم الآلي اللازمة لمراقبة سجلات الأحداث.

١-٥ يجب مراقبة جميع نقاط التحكم بالدخول (Access Control Points) بين حدود الشبكة والاتصالات الخارجية.

١-٦ يجب مراقبة جميع أحداث الأمن السيبراني على مدار الساعة (٣٦٥/٧/٢٤) عن طريق فرق متخصصة.

١-٧ يجب متابعة حسابات التواصل الاجتماعي ومتابعة محاولات تسجيل الدخول لضمان عمل الأنظمة على مدار الساعة وجمع السجلات ذات العلاقة .

١-٨ يجب أن تفعّل الأنظمة المراد مراقبتها سجلات الأحداث عند وقوع أحد الأحداث، بحد أدنى ما يلي:

١-٨-١ الأحداث الخاصة بالأمن السيبراني على جميع المكونات التقنية للأنظمة المراد مراقبتها ومنها أنظمة التشغيل وقواعد البيانات والتخزين والتطبيقات والشبكات.

١-٨-٢ الأحداث الخاصة بالأمن السيبراني للشبكة الصناعية والاتصالات المرتبطة بها.

١-٨-٣ الأحداث الخاصة بالحسابات التي تمتلك صلاحيات مهمة وحساسة على الأصول المعلوماتية.

١-٨-٤ الأحداث الخاصة بالتصفح (DNS Logs) والاتصال بالإنترنت، والشبكة اللاسلكية.

١-٨-٥ الأحداث الخاصة بعمليات الدخول عن بعد.

١-٨-٦ الأحداث الخاصة بخدمات الحوسبة السحابية والاستضافة.

١-٨-٧ الأحداث الخاصة بنقل المعلومات عبر وسائط التخزين الخارجية.

١-٨-٨ الأحداث الخاصة بإجراء تغييرات على السجلات، وملفات الأنظمة الحساسة من خلال تقنيات إدارة تغييرات الملفات (File Integrity Management "FIM").

١-٨-٩ الأحداث الخاصة بتغيير إعدادات النظام، أو الشبكة، أو الخدمات، بما في ذلك تنزيل حزم التحديثات والإصلاحات، أو غيرها من التغييرات على البرامج المثبتة.

١-٨-١٠ الأحداث الخاصة بأنشطة مشبوهة، مثل الأنشطة التي يكتشفها نظام منع التسلل (Intrusion Prevention System "IPS").

١-٨-١١ الأحداث الخاصة بسلوك المستخدم (User Behavior Analytics "UBA") وتحليله.

١-٨-١٢ الأحداث الخاصة بمحاولات الوصول المتعددة وغير الناجحة.

١-٨-١٣ الأحداث الخاصة باتصال أجهزة جديدة، أو غير مسموح بها بشبكات الأنظمة الحساسة وأنظمة التحكم الصناعي (OT/ICS).

اختر التصنيف

الإصدار <١,٠>

٩-١ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

الأدوار والمسؤوليات

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

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

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

٤- **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

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذه السياسة بشكل دوري.

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

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