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

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج سياسة إدارة حوادث وتهديدات 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 "<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.

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 <١,٠>

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 <١,٠>

قائمة المحتويات

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بإدارة حوادث وتهديدات الأمن السيبراني 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 الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة>، وتنطبق هذه السياسة على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب على <اسم الجهة> توفير التقنيات اللازمة لتحديد حوادث الأمن السيبراني واكتشافها في الوقت المناسب أو من خلال استلام البلاغات من العاملين أو المستفيدين من خدمات <اسم الجهة> وإدارتها بشكل فعال.

١-٢ يجب على <اسم الجهة> التعامل مع تهديدات الأمن السيبراني استباقياً باعتماد وسائل الدفاع الوقائية لمنع أو تقليل الآثار المترتبة على سرية المعلومات أو سلامتها أو توافرها.

١-٣ يجب توثيق واعتماد خطة استجابة للحوادث توضح إجراءات التعامل مع حوادث الأمن السيبراني، والأدوار والمسؤوليات الخاصة بفريق الاستجابة، وصلاحيات اتخاذ القرارات الهامة، وآلية التواصل مع الجهات الداخلية والخارجية وكذلك آليات التصعيد.

١-٤ يجب اختبار قدرات الاستجابة لحوادث الأمن السيبراني ومستوى الجاهزية والخطة المعتمدة بشكل دوري من خلال إجراء تمارين محاكاة للهجمات السيبرانية (Attack Simulation Exercises).

١-٥ يجب تزويد العاملين بالجهة بالمهارات والدورات التدريبية المطلوبة (الموظفين والمتعاقدين)، للاستجابة لحوادث الأمن السيبراني بشكل فعال.

١-٦ تشمل حوادث الأمن السيبراني على سبيل المثال لا الحصر ما يلي:

١-٦-١ التغييرات غير المصرح بها في إعدادات أجهزة المستخدمين المكتبية و/أو المحمولة، والتغييرات في إعدادات الخوادم.

١-٦-٢ البرمجيات الضارة.

١-٦-٣ التغييرات في التطبيقات من حيث المظهر (المظهر غير الاعتيادي) والتعديلات على صلاحيات المستخدم.

١-٦-٤ الوصول غير المصرح به إلى البيانات أو تعديلها دون تصاريح أو صلاحيات المستخدمين.

١-٦-٥ محاولات الحصول على معلومات يمكن استخدامها في تنفيذ الهجمات، مثل فحص منافذ الشبكة (Port Scans)، والهندسة الاجتماعية (Attacks Social Engineering)، وفحص مجال شبكة محددة (Targeted Scans Across IP Range)، وغيرها.

١-٦-٦ التفعيل غير المصرح به لحسابات مستخدمين موقوفة أو محذوفة.

١-٧ يجب مواءمة خطط الاستجابة لحوادث الأمن السيبراني مع خطط الاستجابة لحوادث تقنية المعلومات وإدارة الأزمات وخطط استمرارية الأعمال.

١-٨ في حالة العمل عن بعد، يجب تحديث خطط الاستجابة لحوادث الأمن السيبراني ومعلومات التواصل داخل الجهة بما يتوافق مع حالة العمل عن بعد، وبما يضمن القدرة على التواصل وجاهزية فرق الاستجابة للحوادث.

١-٩ في حال اكتشاف حادثة أمن سيبراني في <اسم الجهة>، يجب على فريق الاستجابة للحوادث اتخاذ الخطوات اللازمة للتعامل مع الحادثة التي تم اكتشافها فوراً والتي تشمل تحليل بيانات الحادثة وتحديد أثرها.

١-١٠ في حال اكتشاف حادثة أمن سيبراني، يجب تحليل المعلومات المتاحة ذات العلاقة مثل سجلات النظام والشبكة، والسجلات الصادرة من المنتجات الأمنية ذات الصلة (مثل السجلات الصادرة من حلول الحماية من البرمجيات الضارة، ومن جدار الحماية، ومن أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات).

١-١١ يجب جمع الأدلة اللازمة (على سبيل المثال لا الحصر، جمع الأدلة وفقاً للقيود القانونية وحمايتها من التلاعب) وينبغي توثيقها وحفظها بصورة محمية حتى لا تفقد جدواها في التحليل، ثم تحليلها دون تدميرها أو تعديل صورتها الأصلية.

١-١٢ في حال وقوع حادثة أمن سيبراني، يجب التحقيق في أسباب حدوثها والاستعانة بالمختصين مثل خبراء التحليل الجنائي الرقمي (Digital Forensics Analysts) وفرق الاستجابة للحوادث السيبرانية.

١-١٣ يجب مراجعة خطط الاستجابة للحوادث والقدرات ومدى الجاهزية للاستجابة للحوادث، مرة واحدة في السنة؛ على الأقل.

١-١٤ يجب تصنيف حوادث الأمن السيبراني بناءً على مستوى خطورتها ومدى تأثيرها على أعمال <اسم الجهة>

١-١٥ يتم تصنيف حوادث الأمن السيبراني وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة بحسب الجدول أدناه:

جدول ١: تصنيف حوادث الأمن السيبراني

مستوى الخطورة	الوصف	الوقت المستهدف للاستجابة	الوقت المستهدف لحل الحادثة
حادثة كارثية	أعطالًا كارثية للخدمات أو تأثير سلبي على الأمن السيبراني الوطني بحيث تؤدي إلى أو تهدد بإحداث مضاعفات اقتصادية أو اجتماعية خطيرة أو تؤدي لفقدان حياة بعض الأشخاص.	<يحدد من قِبل الجهة> فوراً	<يحدد من قِبل الجهة> فوراً
حادثة حرجة	ضرر جسيم يؤثر بشكل مباشر على سمعة <اسم الجهة> ومصداقيتها، أو يؤثر على العديد من وحدات الأعمال الوظيفية فيها أو موقع الأعمال بصورة كبيرة، مما يستدعي تفعيل إجراءات استمرارية الأعمال.	<يحدد من قِبل الجهة> فوراً	<يحدد من قِبل الجهة> ساعتان
حادثة مرتفعة	انقطاع كبير يؤثر على وحدات الأعمال الوظيفية أو الخدمات الرئيسية أو الموقع.	<يحدد من قِبل الجهة> ساعة أو ساعتان	<يحدد من قِبل الجهة> ٤-٥ ساعات
حادثة متوسطة	تأثير متوسط في سير عمل وحدات الأعمال الوظيفية أو المواقع أو أصول تقنية المعلومات، إضافة إلى تأثير يتراوح ما بين المتوسط والمرتفع على وحدات الأعمال غير الهامة في <اسم الجهة>.	<يحدد من قِبل الجهة> ٢-٣ ساعات	<يحدد من قِبل الجهة> ٨-٩ ساعات
حادثة محدودة	تأثير بسيط على عدد قليل من الموارد، ويمكن تحمل الحادثة لفترة معينة من الزمن.	<يحدد من قِبل الجهة> ٥ ساعات	<يحدد من قِبل الجهة> ٢٤ ساعة

١-١٦ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات إدارة حوادث وتهديدات الأمن السيبراني.

٢- الإبلاغ عن حوادث الأمن السيبراني

٢-١ يجب رفع الوعي الأمني للعاملين في <اسم الجهة> وتوضيح مسؤولياتهم تجاه حوادث الأمن السيبراني أو التهديدات، وذلك للإبلاغ فوراً عن أي حوادث أو تهديدات متعلقة بالأمن السيبراني.

٢-٢ يجب ان تحدد <اسم الجهة> جهة اتصال داخلية للإبلاغ عن الحوادث سواءً عن طريق الهاتف أو البريد الإلكتروني.

٢-٣ يجب أن تحدد <اسم الجهة> الحوادث والتهديدات التي يجب الإبلاغ عنها ووقت الإبلاغ عنها والأطراف التي يجب إبلاغها، مثل <صاحب الصلاحية> و<رئيس الإدارة المعنية بالأمن السيبراني> وفرق الاستجابة للحوادث داخل <اسم الجهة> والإدارات المسؤولة عن الأصول المعلوماتية والتقنية.

اختر التصنيف

الإصدار <١,٠>

٢-٤ قبل الإفصاح عن أي معلومات متعلقة بالحوادث الأمنية إلى أطراف خارجية، يجب الحصول على الموافقات اللازمة بما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٥ يجب إبلاغ الهيئة الوطنية للأمن السيبراني عن حوادث الأمن السيبراني فور حدوثها.

٢-٦ يجب مشاركة تقارير الحوادث ومؤشرات وتقارير الاختراق مع الهيئة الوطنية للأمن السيبراني.

٣- الاستجابة للحوادث والتعافي من حوادث الأمن السيبراني

٣-١ يجب على فريق الاستجابة للحوادث في <اسم الجهة> كتابة تقرير مفصل عن حوادث الأمن السيبراني، ويجب أن يشمل التقرير نوع الحادثة وتصنيفها والعاملين الذين أبلغوا عن الحادثة أو الأدوات المستخدمة في اكتشافها، والخدمات أو الأصول أو المعلومات المتأثرة بها، وكيفية اكتشاف الحادثة، وأي وثائق أو موارد أخرى متعلقة بالحادثة.

٣-٢ يجب تحليل وتحديث الأسباب الجذرية (Root Cause Analysis) لحوادث الأمن السيبراني ووضع خطط لمعالجتها.

٣-٣ يجب أن يتم إشراك الموردين في حل الحوادث أو استعادة الخدمات عند الحاجة.

٣-٤ يجب تنفيذ وتطبيق التوصيات والتنبيهات الخاصة بحوادث وتهديدات الأمن السيبراني الصادرة من مشرف القطاع أو الهيئة الوطنية للأمن السيبراني.

٣-٥ يجب أن تتضمن إجراءات التعافي من حوادث الأمن السيبراني تحديد الثغرات التي تم استغلالها خلال الحادثة ومعالجتها بالتدابير الفنية والإدارية اللازمة، على سبيل المثال لا الحصر:

٣-٥-١ تطبيق الضوابط الأمنية الإضافية (Compensating Controls).

٣-٥-٢ تنصيب حزم التحديثات والإصلاحات المحدثة.

٣-٥-٣ استعادة النسخ الاحتياطية للنظام.

٣-٥-٤ إعادة ضبط إعدادات الأنظمة الأمنية، مثل نظام جدار الحماية وأنظمة الكشف عن الاختراق.

٣-٦ يجب على <اسم الجهة> حفظ تقارير الحادثة (التي تتضمن معلومات حول الاختراقات الأمنية والحوادث مثل المعلومات المتعلقة بالأفراد والإدارات وأنظمة معينة و/أو منهجية الهجمات) بمكان آمن وتقييد الوصول إليها.

٣-٧ يجب تصعيد الحادثة، في حال عدم حلها في الوقت الزمني المحدد، وفقاً لتصنيف الحوادث وإجراءات التعامل معها وآلية التصعيد المعتمدة.

٣-٨ في حال تطلبت معالجة حادثة سيبرانية إجراء تغييرات على المكونات التقنية، يجب الالتزام بإجراءات إدارة التغيير المعتمدة لدى <اسم الجهة>.

٣-٩ بعد التعامل مع الحادثة، يجب على فريق الاستجابة للحوادث في <اسم الجهة> عقد اجتماعات لمناقشة الدروس المستفادة (Lessons Learned) مع الإدارات ذات العلاقة لتحسين طرق التعامل مع حوادث الأمن السيبراني في المستقبل، وكذلك التعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال <اسم الجهة>.

٤- المعلومات الاستباقية بشأن التهديدات

٤-١ يجب الاشتراك مع مقدمي المعلومات الاستباقية (Threat Intelligence) للاطلاع المستمر على الحوادث والتهديدات المتعلقة بالأمن السيبراني والتعامل مع تلك المعلومات بشكل مباشر.

٤-٢ يجب حفظ المعلومات الاستباقية بشأن التهديدات وتنظيمها في قاعدة بيانات مرنة وملائمة لصياغة ملاحظات العمل والبيانات الوصفية للمؤشرات، مثل قاعدة المعرفة (Knowledge Base).

٤-٣ يجب تحديث والتأكد من إمكانيات أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention and Detection Systems) بناء على المعلومات الاستباقية المتعلقة بالتهديدات.

٤-٤ يجب الاشتراك مع مقدمي المعلومات الاستباقية (Threat Intelligence) ذات العلاقة بأنظمة العمل عن بعد والتعامل معها بشكل دوري.

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> و<الإدارة المعنية بالأمن السيبراني>.

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 مستمر.

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

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

اختر التصنيف

الإصدار <١,٠>