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

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

متاح

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

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حوادث وتهديدات الأمن السيبراني الخاصة بـ<اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية 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 ٢-١٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

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

بنود السياسة

1- المتطلبات العامة

1-1 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.

2-1 يجب على <اسم الجهة> التعامل مع تهديدات الأمن السيبراني استباقياً باعتماد وسائل دفاع وقائية من أجل منع أو تقليل الآثار المترتبة على سرية المعلومات أو سلامتها أو توافرها.

3-1 تشمل حوادث الأمن السيبراني على سبيل المثال لا الحصر ما يلي:

1-3-1 التغييرات غير المصرح بها في إعدادات أجهزة المستخدمين المكتبية و/أو المحمولة، والتغييرات في إعدادات الخوادم.

2-3-1 الإصابة بالبرمجيات الضارة.

3-3-1 التغييرات في التطبيقات من حيث المظهر (المظهر غير الاعتيادي) والتعديلات على صلاحيات المستخدم مثل رفع مستوى الوصول.

4-3-1 الوصول غير المصرح به إلى البيانات، و/أو تعديلها دون تصاريح أو صلاحيات المستخدمين.

5-3-1 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.

6-3-1 التفعيل غير المصرح به لحسابات مستخدمين موقوفة أو محذوفة.

4-1 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. (ECC-2-13-3-1)

5-1 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.

6-1 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).

7-1 يجب معالجة الأدلة اللازمة (على سبيل المثال، 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.

8-1 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.

9-1 يجب مراجعة خطة الاستجابة للحوادث مرة واحدة في السنة؛ على الأقل.

10-1 يجب تصنيف حوادث الأمن السيبراني بناءً على مستوى خطورتها ومدى تأثيرها على أعمال <اسم الجهة>. (ECC-2-13-3-2)

11-1 يتم تصنيف حوادث الأمن السيبراني وفقاً للجدول أدناه:

جدول 1: تصنيف حوادث الأمن السيبراني

مستوى الخطورة	الوصف	الوقت المستهدف للاستجابة	الوقت المستهدف لحل الحادثة
مرتفع جداً	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
مرتفع	انقطاع كبير يؤثر على وحدات الأعمال الوظيفية أو الخدمات الرئيسية أو الموقع.	<يحدد من قِبل الجهة> ساعة أو ساعتان	<يحدد من قِبل الجهة> 5-4 ساعات
متوسط	تأثير متوسط في سير عمل وحدات الأعمال الوظيفية أو المواقع أو أصول تقنية المعلومات، إضافة إلى تأثير يتراوح	<يحدد من قِبل الجهة> 3-2 ساعات	<يحدد من قِبل الجهة> 9-8 ساعات

اختر التصنيف

مستوى الخطورة	الوصف	الوقت المستهدف للاستجابة	الوقت المستهدف لحل الحادثة
	ما بين المتوسط والمرتفع على وحدات الأعمال غير الهامة في <اسم الجهة>.		
منخفض	تأثير بسيط على عدد قليل من الموارد، ويمكن تحمل الحادثة لفترة معينة من الزمن.	<يحدد من قِبل الجهة> 5 ساعات	<يحدد من قِبل الجهة> 24 ساعة

2- الإبلاغ عن حوادث الأمن السيبراني

2-1 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.

2-2 يجب على <اسم الجهة> تحديد جهة اتصال داخلية للإبلاغ عن الحوادث سواءً عن طريق الهاتف أو البريد الإلكتروني.

2-3 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.

2-4 قبل الإفصاح عن أي معلومات متعلقة بالحوادث الأمنية إلى أطراف خارجية، يجب الحصول على الموافقات اللازمة بما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

2-5 يجب إبلاغ الهيئة الوطنية للأمن السيبراني عن حوادث الأمن السيبراني. (ECC-2-13-3-3)

2-6 يجب على <اسم الجهة> إطلاع الهيئة الوطنية للأمن السيبراني على تبليغات الحوادث ومؤشرات وتقارير الانتهاكات. (ECC-2-13-3-4)

3- الاستجابة للحوادث والتعافي من حوادث الأمن السيبراني

3-1 يجب على فريق الاستجابة للحوادث في <الإدارة المعنية بالأمن السيبراني> كتابة تقرير مفصل عن حوادث الأمن السيبراني، ويجب أن يشمل التقرير نوع الحادثة وفئتها 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.

3-2 يجب أن يتم إشراك الموردين في حل الحوادث أو استعادة الخدمات عند الحاجة.

3-3 يجب أن تتضمن إجراءات التعافي من حوادث الأمن السيبراني تحديد الثغرات التي تم استغلالها خلال الحادثة ومعالجتها بالتدابير الفنية والإدارية اللازمة، على سبيل المثال:

3-3-1 تطبيق الضوابط الأمنية الإضافية (Compensating Controls).

3-3-2 تنصيب حزم التحديثات والإصلاحات المحدثة.

3-3-3 استعادة النسخ الاحتياطية للنظام.

4-3-3 إعادة ضبط إعدادات الأنظمة الأمنية، مثل نظام جدار الحماية وأنظمة الكشف عن الاختراق.

4-3 يجب على <الإدارة المعنية بالأمن السيبراني> 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.

5-3 يجب تصعيد الحادثة، في حال عدم حلها في الوقت الزمني المحدد، وفقاً لتصنيف الحوادث وإجراءات التعامل معها وآلية التصعيد المعتمدة.

6-3 في حال تطلبت معالجة حادثة سيبرانية إجراء تغييرات على المكونات التقنية، يجب الالتزام بإجراءات إدارة التغيير المعتمدة لدى <اسم الجهة>.

7-3 بعد التعامل مع الحادثة، يجب على فريق الاستجابة للحوادث في <الإدارة المعنية بالأمن السيبراني> 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>.

4- المعلومات الاستباقية بشأن التهديدات

1-4 يجب الاشتراك مع مقدمي المعلومات الاستباقية (Threat Intelligence) للاطلاع المستمر على الحوادث والتهديدات المتعلقة بالأمن السيبراني والتعامل مع تلك المعلومات بشكل مباشر. (ECC-2-13-3-5)

2-4 يجب حفظ المعلومات الاستباقية بشأن التهديدات وتنظيمها في قاعدة بيانات مرنة وملائمة لصياغة ملاحظات العمل والبيانات الوصفية للمؤشرات، مثل قاعدة المعرفة (Knowledge Base).

3-4 يجب تحديث أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention and Detection Systems) بالمعلومات الاستباقية المتعلقة بالتهديدات والتأكد من إمكانية تلك الأنظمة من اكتشاف التهديدات والتعامل معها بشكل فعال.

5- متطلبات أخرى

1-5 يجب مراجعة متطلبات الأمن السيبراني الخاصة بإدارة حوادث وتهديدات الأمن السيبراني دورياً. (ECC-2-13-4)

2-5 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة حوادث وتهديدات الأمن السيبراني.

3-5 يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

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 مستمر.

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>.