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 مخاطر الأمن السيبراني

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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.

اعتماد الوثيقة

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

نسخ الوثيقة

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

قائمة المحتويات

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لإدارة مخاطر الأمن السيبراني في <اسم الجهة>، وذلك وفقاً لاعتبارات سرية الأصول المعلوماتية والتقنية وتوافرها وسلامتها.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضابط رقم ١-٥-١ 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 وأنظمة وأجهزة التحكم الصناعي الخاصة بـ<اسم الجهة> وإجراءات عمل <اسم الجهة>، وتنطبق على جميع العاملين في <اسم الجهة>.

بنود السياسة

1- البنود العامة

1-1 يجب تطوير وتوثيق واعتماد منهجية إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management Methodology) وإجراءات إدارة مخاطر الأمن السيبراني في <اسم الجهة>، ويجب مواءمتها مع الإطار الوطني لمخاطر الأمن السيبراني (National Cybersecurity Risk Management Framework) ويمكن استخدام المعايير والأطر التوجيهية المعتمدة دولياً (مثل: ISO27005، وISO31000، وNIST) في تطوير منهجية إدارة مخاطر الأمن السيبراني.

2-1 يجب أن تغطي منهجية إدارة مخاطر الأمن السيبراني بحد أدنى ما يلي:

1-2-1 تحديد الأصول ومعرفة أهميتها.

2-2-1 تحديد وتقييم المخاطر التي تمس أعمال أو أصول أو العاملين في <اسم الجهة> (مثل: الآثار المترتبة على <اسم الجهة> الناتجة عن المخاطر السيبرانية).

3-2-1 تحديد التهديدات والثغرات المتعلقة بالأمن السيبراني التي قد تؤثر على الأصول المعلوماتية والتقنية وتقييمها.

4-2-1 تحديد أساليب التعامل مع المخاطر السيبرانية.

5-2-1 ترتيب تدابير الحدّ من المخاطر السيبرانية حسب الأولية ووفق إجراءات محدّدة.

6-2-1 تصنيف مستويات المخاطر السيبرانية وتعريفها بناءً على مستوى التأثير واحتمالية حدوث التهديد لـ<اسم الجهة>.

7-2-1 إنشاء سجل مخاطر الأمن السيبراني لتوثيق المخاطر ومتابعتها.

8-2-1 تحديد الأدوار والمسؤوليات لإدارة مخاطر الأمن السيبراني والتعامل معها.

3-1 يجب تنفيذ تقييم المخاطر دورياً لضمان حماية الأصول المعلوماتية والتقنية والتعامل مع المخاطر حسب الأولوية.

4-1 يجب أن تكون إدارة مخاطر الأمن السيبراني متوافقة مع إدارة المخاطر المؤسسية (Enterprise Risk Management "ERM") في <اسم الجهة>.

2- المراحل الرئيسية لإدارة المخاطر السيبرانية

1-2 تحديد المخاطر (Risk Identification): يجب أن تُحدّد <الإدارة المعنية بالأمن السيبراني> الأحداث أو الظروف التي من الممكن أن تنتهك سريّة الأصول المعلوماتية والتقنية وسلامتها وتوافرها، ويشمل ذلك على وجه الخصوص تحديد الأصول المعلوماتية والتقنية، والتهديدات التي من المحتمل أن تتعرّض لها والثغرات ذات الصلة، والضوابط المعتمدة، ومن ثمّ تحديد الآثار الناتجة عن فقدان سريّة هذه الأصول وسلامتها وتوافرها.

2-2 تقييم المخاطر (Risk Assessment):

1-2-2 يجب على <الإدارة المعنية بالأمن السيبراني> تنفيذ إجراءات تقييم مخاطر الأمن السيبراني بحد أدنى في الحالات التالية:

1-1-2-2 في المراحل الأولى من المشاريع التقنية.

2-1-2-2 قبل إجراء تغيير جوهري في البنية التقنية.

3-1-2-2 عند التخطيط للحصول على خدمات طرف خارجي.

4-1-2-2 عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة.

2-2-2 يجب إعادة تقييم المخاطر وتحديثها على النحو التالي:

1-2-2-2 دورياً لجميع الأصول المعلوماتية والتقنية، وسنوياً على الأقل للأنظمة الحسّاسة. (CSCC-1-2-1-1)

2-2-2-2 بعد وقوع حادث متعلّق بالأمن السيبراني ينتهك سلامة الأصول المعلوماتية والتقنية وتوافرها وسريّتها.

3-2-2-2 بعد الحصول على نتائج تدقيق مهمّة أو معلومات استباقية.

4-2-2-2 في حال التغيير على الأصول المعلوماتية والتقنية.

3-2-2 يجب أن تغطي عملية تقييم المخاطر ما يلي:

1-3-2-2 تحليل المخاطر (Risk Analysis): يجب أن تُقيّم <الإدارة المعنية بالأمن السيبراني> احتمالية وقوع التهديدات والآثار الناتجة عنها، وأن تستخدم نتائج هذا التقييم لتحديد المستوى العام لهذه المخاطر. ويجب أن تعتمد <الإدارة المعنية بالأمن السيبراني> منهجية كميّة (Quantitative) أو نوعيّة (Qualitative) لإجراء تحليل المخاطر.

2-3-2-2 تقدير المخاطر (Risk Evaluation): يجب أن تُقدِّر <الإدارة المعنية بالأمن السيبراني> حجم المخاطر السيبرانية بالتوافق مع معايير تقدير المخاطر المؤسسية المعتمدة في <اسم الجهة>، وتحديد أساليب التعامل معها حسب الأولوية.

3-2 معالجة المخاطر (Risk Treatment):

1-3-2 يجب أن تحدد <الإدارة المعنية بالأمن السيبراني> خيارات معالجة المخاطر حسب القائمة التالية:

1-1-3-2 معالجة المخاطر أو تقليلها (Risk Mitigation): معالجة أو تقليل درجة الخطر من خلال تطبيق الضوابط الأمنية اللازمة لتقليل احتمال الحدوث أو التأثير أو كليهما، والتي تساعد في احتواء المخاطر والمحافظة عليها ضمن مستويات مقبولة.

2-1-3-2 تجنّب المخاطر (Risk Avoidance): التخلص من الخطر بتجنب الاستمرار بمصدر الخطر.

1-2-1-3-2 مشاركة المخاطر أو تحويلها (Risk Transfer): مشاركة المخاطر مع طرف ثالث لديه الإمكانيات في التعامل مع المخاطر بشكل أكثر فعالية، أو التأمين على الأصول المعلوماتية والتقنية في حال تعرضها لمخاطر سيبرانية.

2-2-1-3-2 تقبّل المخاطر وتحمّلها (Risk Acceptance): مستوى الخطر مقبول ولكن يجب المراقبة باستمرار في حال حدوث تغيير.

2-3-2 يجب تحديد خيارات معالجة المخاطر وتوثيقها بناءً على نتائج تقييم المخاطر وتكلفة التنفيذ والمنافع المتوقّعة.

4-2 متابعة المخاطر (Risk Oversight):

1-4-2 لمتابعة المخاطر يجب أن تُعِدّ <الإدارة المعنية بالأمن السيبراني> سجلاً للمخاطر وأن تحافظ عليه لتوثيق مخرجات عملية إدارة المخاطر. على أن يشمل بحد أدنى على المعلومات التالية:

1-1-4-2 عملية تحديد المخاطر.

2-1-4-2 نطاق المخاطر.

3-1-4-2 المسؤول أو صاحب المخاطر.

4-1-4-2 وصف للمخاطر بما في ذلك أسبابها وآثارها.

5-1-4-2 تحليل للمخاطر يُوضّح التأثيرات الناتجة عن المخاطر ونطاقها الزمني.

6-1-4-2 تقييم وتصنيف للمخاطر يشتمل على احتمالية المخاطر وحجمها وتصنيفها الإجمالي في حال حدوثها.

7-1-4-2 خطّة التعامل مع المخاطر تتضمّن إجراء التعامل معها والشخص المسؤول عنها وجدولها الزمني.

8-1-4-2 وصف الخطر المتبقي.

2-4-2 يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان فعالية إدارة مخاطر الأمن السيبراني.

3-4-2 يجب على <الإدارة المعنية بالأمن السيبراني> جمع الأدلة المتعلقة بحالة المخاطر السيبرانية ومراجعتها بشكل دوري.

اختر التصنيف

3- مستوى المخاطر المقبول (Risk Appetite)

3-1 يجب تحديد معايير تقبّل المخاطر وتوثيقها، وفقاً لمستوى المخاطر وتكلفة معالجة الخطر مقابل تأثيره.

3-2 يجب تطبيق ضوابط إضافية من أجل تقليل المخاطر إلى مستوى مقبول في حال عدم استيفاء الخطر المتبقي لمعايير تقبّل المخاطر.

3-3 في حال تجاوز معايير تقبّل المخاطر، يتم التصعيد لصاحب الصلاحية لاتخاذ الإجراءات أو القرارات اللازمة.

4- متطلبات أخرى

4-1 يجب مراجعة منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتحديثها على فترات زمنية مخطط لها (أو في حال حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة)، كما يجب توثيق التغييرات واعتمادها.

4-2 يجب مراجعة سياسة إدارة مخاطر الأمن السيبراني سنوياً، وتوثيق التغييرات واعتمادها.

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 بالأمن السيبراني>.

الالتزام بالسياسة

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

2- يجب على جميع 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>.