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 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.

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	عُدلَ 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

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المتعلقة بإدارة مخاطر الأمن السيبراني في <اسم الجهة> لتحقيق الغرض الأساسي من السياسة وهو تقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية في <اسم الجهة>. هذه المتطلبات تمت موائمتها مع متطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني ويشمل ذلك على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC ٢٠١٨ :١ –)، ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – ١: ٢٠١٩) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل

تطبق هذه السياسة على جميع الأصول المعلوماتية والتقنية والأنظمة الخاصة ب<اسم الجهة> وإجراءات عمل <اسم الجهة>، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب توثيق وتطوير واعتماد منهجية إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management Methodology) وإجراءات إدارة مخاطر الأمن السيبراني في <اسم الجهة>، على أن يتم التأكد من مواءمتها مع الإطار الوطني لإدارة مخاطر الأمن السيبراني (National Cybersecurity Risk Management Framework) والذي بدوره تمت مواءمته مع المعايير والأطر التوجيهية المعتمدة دوليًا (مثل: ISO٢٧٠٠٥، وISO٣١٠٠٠، وNIST).

١-٢ يجب أن تغطي منهجية إدارة مخاطر الأمن السيبراني بحد أدنى ما يلي:

١-٢-١ تحديد وجمع، وإعداد قائمة للأصول، وتصنيف الأصول وترتيبها حسب الأولوية في الحماية.

١-٢-٢ تحديد وتقييم المخاطر التي تمس أعمال أو أصول أو العاملين في <اسم الجهة> (مثل: الآثار المترتبة على <اسم الجهة> الناتجة عن المخاطر السيبرانية).

١-٢-٣ تقييم المخاطر السيبرانية عند التخطيط وقبل السماح باستخدام شبكات التواصل الاجتماعي وقبل السماح بالعمل عن بعد لأي خدمة أو نظام.

١-٢-٤ تحديد التهديدات والثغرات المتعلقة بالأمن السيبراني التي قد تؤثر على الأصول المعلوماتية والتقنية وتقييمها.

١-٢-٥ تحديد قرار الاستجابة للمخاطر السيبرانية.

١-٢-٦ ترتيب خطط الاستجابة للمخاطر السيبرانية حسب الأولوية ووفق إجراءات محدّدة.

١-٢-٧ تصنيف مستويات المخاطر السيبرانية وتعريفها بناءً على مستوى التأثير واحتمالية حدوث التهديد لـ<اسم الجهة>.

١-٢-٨ تحديد الأدوار والمسؤوليات لإدارة مخاطر الأمن السيبراني والتعامل معها.

١-٣ يجب تنفيذ تقييم المخاطر دوريًا لضمان حماية الأصول المعلوماتية والتقنية والتعامل مع المخاطر حسب الأولوية.

١-٤ يجب ضمان إدارة مخاطر الأمن السيبراني على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية في <اسم الجهة>.

١-٥ يجب المتابعة والمراقبة الدائمة المستمرة للمخاطر السيبرانية في <اسم الجهة>.

١-٦ يجب أن تكون إدارة مخاطر الأمن السيبراني متوافقة مع إدارة المخاطر المؤسسية (Risk Management "ERM" Enterprise) في <اسم الجهة>.

١-٧ يجب تطبيق التوصيات الصادرة عن الهيئة، فيما يتعلق بإدارة مخاطر الأمن السيبراني.

١-٨ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات إدارة مخاطر الأمن السيبراني.

٢- المراحل الرئيسة لإدارة مخاطر الأمن السيبراني

٢-١ تحديد المخاطر (Risk Identification):

يجب أن تغطي عملية تحديد المخاطر مايلي:

٢-١-١ حصر الأصول، وإعداد قائمة بالأصول مصنفة ومرتبة حسب الأولوية.

٢-١-٢ تحديد وحصر التهديدات والثغرات المحتملة على الأصول التي تم تحديدها.

٢-١-٣ تحديد المخاطر السيبرانية الحالية على الأصول من خلال:

٢-١-٣-١ تطوير السيناريوهات المتوقعة للمخاطر السيبرانية وفقًا للتهديدات والثغرات والهجمات المحتملة.

٢-١-٣-٢ تحديد ضوابط الأمن السيبراني المطبقة حاليًا لمواجهة المخاطر السيبرانية.

٢-٢ تقييم المخاطر (Risk Assessment):

٢-٢-١ يجب على <الإدارة المعنية بالأمن السيبراني> تنفيذ إجراءات تقييم المخاطر السيبرانية بحد أدنى في الحالات التالية:

٢-٢-١-١ كل ٣ سنوات على الأقل لجميع الأصول المعلوماتية والتقنية، وسنويًا على الأقل للأنظمة الحسّاسة ولأنظمة العمل عن بعد ولحسابات التواصل الاجتماعي.

٢-٢-١-٢ في المراحل الأولى من المشاريع التقنية.

٢-٢-١-٣ قبل إجراء تغيير جوهري في البنية التقنية.

٢-٢-١-٤ عند التخطيط للحصول على خدمات طرف خارجي.

٢-٢-١-٥ عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة.

٢-٢-٢ يجب إعادة تقييم المخاطر وتحديثها على النحو التالي:

٢-٢-١ بعد وقوع حادث متعلّق بالأمن السيبراني ينتهك سلامة الأصول المعلوماتية والتقنية وتوافرها وسريّتها.

٢-٢-٢ بعد الحصول على نتائج تدقيق مهمّة أو معلومات استباقية.

٢-٢-٣ في حال التغيير على الأصول المعلوماتية والتقنية.

٢-٢-٣ يجب أن تغطي عملية تقييم المخاطر الحالية ما يلي:

٢-٣-٢-١ **تحليل المخاطر** (Risk Analysis): يجب أن تُقيّم <اسم الجهة> احتمالية وقوع التهديدات والآثار الناتجة عنها، وأن تستخدم نتائج هذا التقييم لتحديد المستوى العام لهذه المخاطر. ويجب أن تعتمد <اسم الجهة> منهجية كميّة (Quantitative) أو نوعيّة (Qualitative) لإجراء تحليل المخاطر.

٢-٣-٢-٢ **تقدير المخاطر** (Risk Evaluation): يجب أن تُقدِّر <اسم الجهة> حجم المخاطر السيبرانية بالتوافق مع معايير تقدير المخاطر المؤسسية المعتمدة في <اسم الجهة>، وتحديد أساليب التعامل معها حسب الأولوية.

٢-٣ الاستجابة للمخاطر الحالية (Risk Response):

٢-٣-١ يجب أن تحدد <اسم الجهة> قرار الاستجابة للمخاطر حسب القائمة التالية:

٢-٣-١-١ **معالجة المخاطر أو تقليلها** (Risk Mitigation): معالجة أو تقليل درجة الخطر من خلال تحديد وتنفيذ خطط الاستجابة اللازمة لتقليل احتمال الحدوث أو التأثير أو كليهما، والتي تساعد في احتواء المخاطر والمحافظة عليها ضمن مستويات مقبولة، ويجب على <اسم الجهة> العمل بالتالي:

- تحديد وتوثيق خطط الاستجابة للمخاطر السيبرانية للتعامل مع المخاطر الحالية، وترتيبها حسب الأولوية.
- تنفيذ خطط الاستجابة للمخاطر السيبرانية حسب الأولوية.
- حساب المخاطر السيبرانية المتبقية بعد تنفيذ خطط الاستجابة للمخاطر.

٢-٣-١-٢ **تجنّب المخاطر** (Risk Avoidance): إزالة الخطر بتجنب الاستمرار بمصدر الخطر.

٢-٣-١-٢-١ 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.

٢-٣-١-٢-٢ تقبّل المخاطر وتحمّلها (Risk Acceptance): مستوى الخطر مقبول ولدى <اسم الجهة> جاهزية لقبوله، ولكن يجب المراقبة باستمرار في حال حدوث تغيير.

٢-٣-٢ يجب تحديد خيارات معالجة المخاطر وتوثيقها بناءً على نتائج تقييم المخاطر وتكلفة التنفيذ والمنافع المتوقّعة.

٢-٤ متابعة المخاطر (Risk Oversight):

٢-٤-١ لمتابعة المخاطر يجب أن تطور <اسم الجهة> سجلًا للمخاطر لتوثيق مخرجات عملية إدارة المخاطر، وتتم مراجعته باستمرار. على أن يشمل بحد أدنى على المعلومات التالية:

٢-٤-١-١ عملية تحديد المخاطر.

٢-٤-١-٢ نطاق المخاطر.

٢-٤-١-٣ مالك المخاطر.

٢-٤-١-٤ وصف للمخاطر بما في ذلك أسبابها وآثارها.

٢-٤-١-٥ تحليل للمخاطر يُوضّح التأثيرات الناتجة عن المخاطر ونطاقها الزمني.

٢-٤-١-٦ تقييم وتصنيف للمخاطر يشتمل على احتمالية المخاطر وحجمها وتصنيفها الإجمالي في حال حدوثها.

٢-٤-١-٧ خطط الاستجابة للمخاطر وتتضمن تتضمّن إجراءات التعامل معها والشخص المسؤول عنها وجدولها الزمني.

٢-٤-١-٨ وصف الخطر المتبقي.

٢-٤-٢ يجب إنشاء سجل للمخاطر السيبرانية خاص بالعمليات وخدمات الحوسبة السحابية والأنظمة الحساسة، ومتابعتها دوريًا بما يتناسب مع طبيعة المخاطر.

٢-٤-٣ يجب تضمين المخاطر السيبرانية الخاصة بأنظمة العمل عن بعد والخدمات والأنظمة المسموح لها بالعمل عن بعد وبحسابات التواصل الاجتماعي والخدمات والأنظمة المستخدمة في ذلك في سجل المخاطر السيبرانية الخاص بالجهة، ومتابعته مرة واحدة سنوياً، على الأقل.

٢-٤-٤ يجب على <اسم الجهة> جمع الأدلة المتعلقة بحالة المخاطر السيبرانية ومراجعتها بشكل سنوي.

٢-٤-٥ يجب تطوير تقارير إدارة مخاطر الأمن السيبراني.

٣- مستوى المخاطر المقبول (Risk Appetite)

٣-١ يجب تحديد مستوى المخاطر المقبول وتوثيقها، وفقًا لمستوى المخاطر وتكلفة معالجة الخطر مقابل تأثيره.

٣-٢ يجب تحديد مستوى المخاطر المقبول فيما يتعلق بخدمات الحوسبة السحابية.

٣-٣ يجب تطبيق ضوابط إضافية من أجل تقليل المخاطر إلى مستوى مقبول في حال عدم استيفاء الخطر المتبقي للمستوى المقبول المخاطر.

٣-٤ في حال تجاوز المستوى المقبول للمخاطر، يتم التصعيد لصاحب الصلاحية لاتخاذ الإجراءات أو القرارات اللازمة.

٤- المخاطر السيبرانية في أنظمة التحكم الصناعي

٤-١ يجب وضع منهجية المخاطر السيبرانية المتعلقة بأنظمة التحكم الصناعي (OT/ICS) ضمن منهجية إدارة المخاطر وإدارة مخاطر السلامة وإجراءاتها في <اسم الجهة>.

٤-٢ يجب تقييم المخاطر السيبرانية، لأنظمة التحكم الصناعي (OT/ICS) بشكل دوري، مع التأكد من تضمين مخاطر توقيع العقود والاتفاقيات، مع الأطراف الخارجية المتعلقة بأنظمة التحكم الصناعي و/أو عند حدوث تغييرات بالمتطلبات التشريعية والتنظيمية، ذات العلاقة بوصفها جزء من التقييم.

٤-٣ يجب تضمين سجل المخاطر السيبرانية المتعلقة بأنظمة التحكم الصناعي (OT/ICS) ضمن سجل المخاطر في <اسم الجهة>.

٤-٤ يجب تحديد المستويات الملائمة للمناطق والمرافق التي تحتوي على أنظمة التحكم الصناعي (OT/ICS) بناءً على منهجية معتمدة.

٤-٥ يجب تضمين تحليل نوعي (Qualitative Analysis) للمخاطر السيبرانية ضمن إجراءات تحليل مخاطر العمليات (Process Hazard Analysis) الذي يطبق مع أي تغيير في العمليات، أو إجراءاتها أو في المصانع.

٤-٦ في حال عدم التمكن من استيفاء متطلبات الأمن السيبراني داخل البيئة الخاصة بأنظمة التحكم الصناعي (OT/ICS) فيجب توضيح المبررات اللازمة مع توثيقها واعتمادها من قبل <الجهة المعنية بالأمن السيبراني> وموافقة صاحب الصلاحية.

٤-٧ في حال الموافقة على قبول المخاطر السيبرانية؛ فيجب تحديد الضوابط البديلة لها مع توثيقها واعتمادها من قبل صاحب الصلاحية ومراجعتها من قبل <الإدارة المعنية بالأمن السيبراني>؛ مع التأكد من تطبيقها بفعالية في وقت محدد، مع الاستمرار في تقييم تلك المخاطر ومراجعتها بشكل مستمر.

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 دوريًا.

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>.