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 الأمن السيبراني ضمن استمرارية الأعمال

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	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 <1.0>

قائمة المحتويات

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة باستمرارية الأعمال الخاصة ب<اسم الجهة> لتقليل المخاطر السيبرانية عليها وحمايتها من التهديدات الداخلية والخارجية في <اسم الجهة> 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 في <اسم الجهة>، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

1 البنود العامة

1-1 يجب التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمن السيبراني في <اسم الجهة>.

2-1 يجب إجراء تقييم للمخاطر التي قد تؤثر على استمرارية أعمال <اسم الجهة>.

3-1 يجب معالجة نقاط الضعف لتجنب الحوادث التي قد تؤثر على استمرارية أعمال <اسم الجهة>.

4-1 يجب تحديد المتطلبات التشريعية والتنظيمية الخاصة باستمرارية الأعمال لدى <اسم الجهة>.

5-1 يجب وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال <اسم الجهة>.

6-1 يجب تضمين خطط استمرارية سلاسل التوريد والإمداد ضمن خطط استمرارية أعمال <اسم الجهة>.

7-1 يجب وضع خطط التعافي من الكوارث (Disaster Recovery Plan).

8-1 يجب تضمين حوادث الأمن السيبراني عالية الخطورة ضمن الأسباب الموجبة لتفعيل خطة استمرارية الأعمال في <اسم الجهة>.

9-1 يجب تضمين طرق التواصل الخاصة بفريق الأمن السيبراني في <اسم الجهة> سواءً الداخلية أو الخارجية وتوثيقها.

10-1 يجب تحديد الأدوار والمسؤوليات للأطراف ذات العلاقة باستمرارية الأعمال في <اسم الجهة>.

11-1 يجب وضع خطط تنفيذ ومتابعة المسؤوليات والأعمال الخاصة بالأمن السيبراني خلال الكوارث ولحين عودة الأوضاع لطبيعتها.

12-1 يجب إدارة هويات الدخول والصلاحيات على جميع الأنظمة والبيانات المستضافة في موقع التعافي من الكوارث الخاص ب<اسم الجهة> لضمان عدم الوصول إليها من قبل الأشخاص غير المصرح لهم.

13-1 يجب ضمان تطبيق ضوابط الأمن السيبراني بناء على متطلبات <اسم الجهة> والهيئة الوطنية للأمن السيبراني مثل (ECC-1:2018, CSCC-1:2019) وأفضل الممارسات العالمية في بيئة مركز التعافي من الكوارث التابع ل<اسم الجهة>.

14-1 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات الأمن السيبراني الخاصة باستمرارية الأعمال.

2 الأنظمة الحساسة وأنظمة الحوسبة السحابية

1-2 يجب إجراء تحليل التأثير على الأعمال (Business Impact Analysis) لتحديد الأنظمة الحساسة في <اسم الجهة> ونسخها إلى موقع التعافي من الكوارث.

2-2 يجب إدراج الأنظمة الحساسة ل<اسم الجهة> ضمن خطط التعافي من الكوارث.

3-2 يجب إنشاء مركز للتعافي من الكوارث للأنظمة الحساسة.

4-2 يجب إجراء اختبارات دورية للتأكد من فعالية خطط التعافي من الكوارث للأنظمة الحساسة ل<اسم الجهة> مرة واحدة سنويًا على الأقل.

5-2 يجب تحديد متطلبات النسخ الدوري للأنظمة الحساسة إلى مركز التعافي.

6-2 يجب تطوير وتنفيذ إجراءات التعافي من الكوارث واستمرارية الأعمال المتعلقة بالحوسبة السحابية وتضمين متطلبات ذلك في عقود واتفاقيات <اسم الجهة> مع الأطراف الخارجية ومقدمي الخدمات السحابية.

7-2 يجب إجراء اختبار سنوي للتعافي من الكوارث (Live DR Test) للأنظمة الحساسة متى ما أمكن ذلك.

الأدوار والمسؤوليات

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

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

3- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية باستمرارية الأعمال> و <الإدارة المعنية بتقنية المعلومات> و <الإدارة المعنية بالأمن السيبراني>.

4- **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

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

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

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