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

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

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 ضمن إدارة استمرارية الأعمال لضمان استمرارية أعمال <اسم الجهة> وحمايتها من المخاطر السيبرانية والتهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على هدف التوافر وهو من الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 3-1-1 من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) والضابط رقم 3-1-1 من ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة إدارة استمرارية الأعمال الخاصة بالأمن السيبراني في <اسم الجهة> وتنطبق على جميع العاملين في <اسم الجهة>.

بنود السياسة

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

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

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

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

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

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

7- يجب إدراج الأنظمة الحساسة لـ<اسم الجهة> ضمن خطط التعافي من الكوارث.

8- يجب إنشاء مركز للتعافي من الكوارث للأنظمة الحساسة.

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

10- يجب إجراء اختبار دوري حي للتعافي من الكوارث (Live DR Test) للأنظمة الحساسة.

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

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

13- يجب تحديد متطلبات النسخ الدورية الخاصة بالأنظمة الحساسة لـ<اسم الجهة> إلى مركز التعافي.

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

اختر التصنيف

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

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

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

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

19- يجب تضمين متطلبات خطط التعافي من الكوارث في عقود واتفاقيات <اسم الجهة> مع الأطراف الخارجية ومقدمي الخدمات السحابية.

20- يجب ضمان تطبيق الضوابط الأساسية للأمن السيبراني (ECC-1:2018) في بيئة مركز التعافي من الكوارث التابع لـ<اسم الجهة> مثل: الأمن المادي، أمن الشبكة والبنية التحتية، أمن البيانات والمعلومات، التشفير، إلخ.

21- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني الخاصة باستمرارية أعمال الأمن السيبراني.

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 باستمرارية الأعمال> و <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 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>.