هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. والبنود الملونة باللون الأخضر هي أمثلة يجب حذفها. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج سياسة النسخ الاحتياطية

استبدل <حاسم الجهة> باسم الجهة في مجمل صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

- اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
- أضف "<حاسم 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.

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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.

اختر التصنيف

الإصدار <١,٠>

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 <١,٠>

قائمة المحتويات

الغرض ٤
نطاق السياسة ٤
بنود السياسة ٤
الأدوار والمسؤوليات ٦
التحديث والمراجعة ٦
الالتزام بالسياسة ٦

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بالنسخ الاحتياطية لجميع المعلومات والأصول التقنية في <اسم الجهة> لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية وذلك لتحقيق الأهداف الرئيسية للحماية وهي: سرية المعلومات، وسلامة أنظمة المعلومات، وتوافرها.

تمت موائمة هذه السياسة مع الضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

تطبق هذه السياسة على الأصول المعلوماتية والتقنية (مثل: الأنظمة والبيانات والمعلومات) الخاصة ب<اسم الجهة>، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب أن تحتوي جميع أنظمة تقنية المعلومات (بما في ذلك أنظمة الحوسبة السحابية وأنظمة الدخول والعمل عن بُعد والأنظمة الحساسة) في <اسم الجهة> على عمليات وإجراءات محددة.

١-٢ يتحمل ملاك الانظمة مسؤولية إنشاء عمليات وإجراءات النسخ الاحتياطية المحددة، بمساعدة ممثلي الأعمال.

١-٣ عندما يتم إعداد النسخ الاحتياطية لأصول المعلوماتية (الأنظمة والبيانات والمعلومات) الخاصة ب <اسم الجهة>، يجب على مالك النظام وممثلي <الإدارة القانونية> و<إدارة حماية البيانات> المساعدة في إنشاء عمليات وإجراءات النسخ الاحتياطي المطلوبة.

١-٤ يجب تقييد الوصول المادي والمنطقي إلى النسخ الاحتياطية ووسائط النسخ الاحتياطي (المادية والإلكترونية) والنسخ الاحتياطية المستعادة الخاصة ب<اسم الجهة> على المستخدمين المصرح لهم فقط. علاوة على ذلك، يجب مراجعة الصلاحيات والامتيازات للوصول المادي والمنطقي لهذه الوسائط بشكل منتظم، مرة واحدة على الأقل في السنة.

١-٥ يجب حماية الوصول إلى النسخ الاحتياطية للأنظمة وتخزينها ونقلها، والنسخ الاحتياطية لبيانات المشتركين في خدمات الحوسبة السحابية، والوسائط المستخدمة لهذه النسخ الاحتياطية من التلف أو التعديل أو الوصول غير المصرح به.

١-٦ يجب أن تلبي متطلبات الأمن السيبراني للنسخ الاحتياطي والاحتفاظ بها واستعادتها المتطلبات التشريعية والتنظيمية، ويجب مراجعتها مرة واحدة على الأقل في السنة وفي حال حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات الصلة.

١-٧ يجب استخدام مؤشرات الأداء (KPI) الرئيسية لضمان التحسين المستمر لمتطلبات الأمن السيبراني الخاصة بالنسخ الاحتياطية والاحتفاظ بها واستعادتها.

اختر التصنيف

الإصدار <١,٠>

٢- النسخ الاحتياطية

٢-١ يجب اختبار وسائط النسخ الاحتياطي بشكل منتظم، ومرة واحدة سنويًا على الأقل، للتأكد من مطابقتها للمواصفات المذكورة من قبل الجهة المصنعة، وخلوها من الأعطال المادية، وأن وظائفها تعمل على النحو المقصود منها، واستبدالها عند الحاجة.

٢-٢ يجب إجراء عمليات النسخ الاحتياطي على فترات منتظمة لتلبية المتطلبات التشريعية والتنظيمية وعلى النحو المحدد في <اسم الجهة>.

٢-٣ يجب عمل تقييم تحليل تأثير انقطاع الأعمال لتحديد وتيرة ونوع النسخ الاحتياطي المطلوب لكل نظام.

٢-٤ يجب عمل نسخ احتياطية يومية لجميع مكونات الأنظمة الحساسة.

٢-٥ يجب أن يغطي النسخ الاحتياطي جميع مكونات الأنظمة الحساسة، سواءً كان نسخًا احتياطيًا عبر اتصال آمن (الذي يستخدم نظام التخزين عن بُعد أو على الحوسبة السحابية للحصول على البيانات المراد تخزينها في خادم متصل بالشبكة)، أو نسخًا احتياطيًا دون اتصال (والذي يستخدم قطعة مادية من الأجهزة مثل القرص الصلب الخارجي أو أقراص الفيديو الرقمية DVD أو بطاقة الذاكرة وما إلى ذلك المعزولة عن أي شبكة أو جهاز متصل بالإنترنت لتخزين البيانات).

٢-٦ يجب تخزين وسائط النسخ الاحتياطي المادية وغير المتصلة بالشبكة خارج الموقع في موقع آمن ومعتمد، ويفضل أن يكون ذلك في موقع بعيد ماديًا.

٢-٧ يجب تخزين النسخ الاحتياطية عبر الإنترنت بشكل منفصل عن بيئات وشبكات الإنتاج والاختبار والتطوير والمكاتب والتقنيات التشغيلية.

٣- الاحتفاظ بالنسخ الاحتياطية

٣-١ يجب الاحتفاظ بالنسخ الاحتياطية الخاصة بـ<اسم الجهة> لفترات زمنية محددة وفقًا لما تتطلبه التشريعات والأنظمة وسياسات الأعمال (مثل: <معيار تصنيف المعلومات> و<معيار الاحتفاظ بالبيانات> واحتياجات الأعمال.

٣-٢ يجب مراجعة النسخ الاحتياطية في فترات زمنية محددة لضمان تلبيتها لجميع متطلبات الاحتفاظ بها، مثل التشريعات والأنظمة واحتياجات الأعمال.

٤- حذف النسخ الاحتياطية

٤-١ لا يجوز حذف النسخ الاحتياطية إلا بعد الحصول على موافقة المالك.

٤-٢ يجب حذف وسائط النسخ الاحتياطي المادية وإتلافها بشكل آمن عند الحاجة.

٤-٣ يجب حذف وسائط النسخ الاحتياطي عبر الإنترنت وإزالتها بشكل آمن عند الحاجة.

٥- استعادة البيانات

٥-١ يجب إجراء اختبار الاستعادة مرة واحدة سنويًا على الأقل لجميع النسخ الاحتياطية.

٥-٢ يجب إجراء اختبار الاستعادة مرة كل ثلاثة أشهر للنسخ الاحتياطية للأنظمة الحساسة.

٥-٣ يجب إجراء اختبار الاستعادة مرة كل ستة أشهر للنسخ الاحتياطية لأنظمة العمل عن بُعد.

اختر التصنيف

الإصدار <١,٠>

٤-٥ يجب أن تكون <اسم الجهة> قادرة على استعادة النسخة الاحتياطية خلال إطار زمني (RTO) محدد بما يتوائم مع احتياجات أعمالها ووقت التعافي المستهدف ونقطة التعافي المستهدفة.

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> و<الإدارة المعنية بالأمن السيبراني>.

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 جميع 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>.