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 أمن وسائط التخزين

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	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

قائمة المحتويات

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بوسائط التخزين المستخدمة في <اسم الجهة> وتحديد عملية التخلص الآمن منها، وذلك لتقليل المخاطر السيبرانية 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 السياسة

تُطبق هذه السياسة على جميع الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة> وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

1- البنود العامة

1-1 يجب أن تضمن <اسم الجهة> التحكم باستخدام أجهزة تخزين الوسائط المستخدمة من قبل العاملين لحفظ ونقل المعلومات في <اسم الجهة>.

2-1 يجب أن تحدد <اسم الجهة> المواد التي تُعتبر وسائط قابلة للإزالة وأي من تلك الوسائط يُمكن توصيله بنظام معلومات أو جهاز أو شبكة توفير و تخزين البيانات، مثل:

- الوسائط المغناطيسية (مثل محركات الأقراص الدوارة، والأشرطة).
- الوسائط الضوئية (مثل محركات الأقراص الضوئية كمحركات الأقراص المضغوطة (CD-R)، وأقراص الفيديو الرقمية (DVD-R)، وأقراص البلو راي).
- أشباه الموصلات (مثل، محركات الأقراص الصلبة SSD، ومشغلات ذاكرة فلاش، ووحدات الذاكرة الثابتة).

3-1 يجب أن تحظر <اسم الجهة> استخدام أجهزة الوسائط القابلة للإزالة ما لم يكن هناك حاجة عمل تقضي باستخدامها.

4-1 يجب أن تقوم <اسم الجهة> بوضع وتطبيق إجراءات رسمية للموافقة على استخدام الوسائط القابلة للإزالة.

5-1 يجب أن تقوم <اسم الجهة> بالتحكم بأجهزة الوسائط ماديًا وتخزينها بشكل آمن في <اسم الجهة>.

6-1 يجب أن تقوم <اسم الجهة> بحماية أجهزة وسائط التخزين حتى يتم إتلافها أو تطهيرها باستخدام المعدات والتقنيات والإجراءات المعتمدة بالمواءمة مع سياسة التخلص الآمن المعمول بها في <اسم الجهة>.

7-1 يجب أن تقيّد <اسم الجهة> استخدام وسائط التخزين الخارجية وتوفر سبل التعامل الآمن معها.

2- الوصول إلى الوسائط

2-1 يجب أن يكون الوصول إلى وسائط التخزين التالية مقيّدًا بناءً على سياسة إدارة الأصول الخاصة ب<اسم الجهة>:

- <النوع الأول من وسائط التخزين الذي تحدده الجهة (مثل أشرطة النسخ الاحتياطي)>
- <النوع الثاني من وسائط التخزين الذي تحدده الجهة (مثل وسائط التخزين على الخوادم)>
- <النوع الثالث من وسائط التخزين الذي تحدده الجهة (مثل التخزين على الشبكة)>

2-2 يجب تطبيق قيود التوزيع، ومحاذير التعامل، وعلامات الأمان المعمول بها على وسائط التخزين.

3- وسائط التخزين

3-1 يجب تعيين عاملين مخصصين لمراقبة أجهزة الوسائط ماديًا وتخزينها في مواقع محددة خاضعة للمراقبة.

3-2 يجب التأكد من حماية وسائط التخزين حتى إتلافها أو تطهيرها باستخدام إجراءات الموافقة على المعدات، كما يجب التأكد من تحديد إجراءات التعامل مع الوسائط، وتحديد تقنيات الحماية المعتمدة.

4- نقل الوسائط

4-1 يجب حماية الوسائط ومراقبتها خلال نقلها إلى خارج المناطق الخاضعة للرقابة.

4-2 يجب تتبع وسائط التخزين أثناء نقلها خارج المناطق الخاضعة للرقابة.

4-3 يجب توثيق الأنشطة المرتبطة بنقل وسائط التخزين، ويجب أن تقتصر على الموظفين المخولين.

4-4 يجب أن تقوم <اسم الجهة> بإعداد السياسات والإجراءات الخاصة بالنقل الآمن للوسائط المادية وتوثيقها والموافقة عليها وتعميمها وتطبيقها وتقييمها وتحديثها.

4-5 يجب أن تقوم <اسم الجهة> بمراجعة وتحديث السياسات والإجراءات المتعلقة بالنقل الآمن للوسائط المادية مرة واحدة سنويا على الأقل.

5- تطهير الوسائط

5-1 يجب أن تقوم <اسم الجهة> بتطهير الوسائط قبل التخلص منها، أو تحريرها من الرقابة المؤسسية أو تحريرها لإعادة استخدامها وفقًا لمعيار أمن التخزين مع تطبيق المعايير والسياسات التنظيمية والمؤسسية المعمول بها.

5-2 يجب تطبيق آليات فلترة بقوة وسلامة تتناسب مع البيانات و تصنيفها.

6- استخدام الوسائط

6-1 يجب أن تحظر <اسم الجهة> استخدام أنواع وسائط التخزين المحددة من قبل <اسم الجهة> على المعدات المملوكة لـ <اسم الجهة> باستخدام إجراءات حماية أمنية غير معتمدة.

الأدوار والمسؤوليات

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

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

3- **تنفيذ السياسة وتطبيقها:** <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 السياسة أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام

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

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

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.