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 حذف التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج معيار الحماية من فقدان البيانات

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

قائمة المحتويات

الغرض 4
نطاق العمل 4
المعايير 4
الأدوار والمسؤوليات 9
التحديث والمراجعة 9
الالتزام بالمعيار 9

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية ذات العلاقة بمنع فقدان البيانات في <اسم الجهة> وذلك لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية في <اسم الجهة> بغرض تحقيق الأهداف الرئيسية للحماية وهي: سرية المعلومات، وسلامة أنظمة المعلومات، وتوافرها.

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

نطاق العمل

هذا المعيار ينطبق على جميع البيانات الخاصة ب<اسم الجهة>، و وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

1	نوع البيانات والمعلومات وتعريف المتجهات (Data and information type (and vector definition
الهدف	تحديد أنواع البيانات والمعلومات المطلوب مراقبتها والاتجاهات التي يمكن أن تتسرب من خلالها هذه البيانات والمعلومات من الجهة.
المخاطر المحتملة	قد يعني ضعف تعريف، أو عدم تعريف، أنواع البيانات والمعلومات والاتجاهات المطلوب مراقبتها أن منهجيات فقدان البيانات غير مصممة ومنفذة بالشكل الصحيح، مما يسمح بتسرب البيانات والمعلومات من <اسم الجهة>.
الإجراءات المطلوبة	
1-1	تحديد أنواع البيانات والمعلومات المطلوب مراقبتها من قبل مالكي الأصول و<رئيس الإدارة المعنية بالأمن السيبراني> مع مدخلات من الجهات المعنية الأخرى في <اسم الجهة>.
2-1	يجب أن يشمل نوع البيانات والمعلومات المطلوب مراقبتها ما يلي: أ) جميع البيانات والمعلومات التي تجب مراقبتها بسبب الالتزامات القانونية والتنظيمية المطبقة على <اسم الجهة> ب) جميع البيانات والمعلومات المصنفة على أنها "مقيدة" أو أعلى (راجع سياسة تصنيف البيانات)

	ت) جميع البيانات والمعلومات التي تعتبر شخصية ث) جميع البيانات والمعلومات التي يجب مراقبتها للوفاء بالالتزامات التشغيلية والتجارية مع الأطراف الخارجية والموردين
3-1	تحديد وتوثيق واعتماد سجل منع فقدان البيانات لأنواع البيانات والمعلومات المطلوب مراقبتها.
4-1	مراجعة الالتزامات القانونية والتنظيمية والتشغيلية والتجارية المفروضة على <اسم الجهة> مرة واحدة سنويًا على الأقل.
5-1	تحديث سجل منع فقدان البيانات والمعلومات المطلوب مراقبتها عند الضرورة لتعكس التغييرات المحددة في المراجعة.
6-1	التحقيق في المتجّهات التي يمكن من خلالها نقل/خروج البيانات والمعلومات من <اسم الجهة>. يجب أن يحدد التحقيق أولويات البيانات والمعلومات المدرجة في سجل منع فقدان البيانات.
7-1	إنشاء وتحديث قائمة بالمتجهات مثل الشبكة (عملاء البريد الإلكتروني وعملاء بروتوكول نقل الملفات وما شابه ذلك) والأنظمة (مسجلات البيانات والطابعات والتخزين القابل للإزالة وما شابه ذلك) والتطبيقات التي يمكن من خلالها تسرب/ نقل البيانات من <اسم الجهة>.
8-1	مراجعة قائمة المتجهات مرة واحدة سنويًا على الأقل.
9-1	تحديث قائمة المتجهات عند الضرورة لتعكس التغييرات المحددة في المراجعة.
2	أداة منع فقدان البيانات (DLP tool (DLP))
الهدف	استخدام أداة منع فقدان البيانات لمراقبة وضبط حركة البيانات والمعلومات المدرجة في سجل منع فقدان البيانات.
المخاطر المحتملة	يؤدي عدم أتمتة مراقبة البيانات والمعلومات إلى ضرورة استخدام <اسم الجهة> العمليات اليدوية (أو عدم استخدام أي عملية على الإطلاق) لتحديد تسرب البيانات والمعلومات وإيقافه، مما يقلل من فعالية وكفاءة منهجيات منع تسرب البيانات
الإجراءات المطلوبة	
1-2	إدارة أداة منع فقدان البيانات مركزيًا.

2-2	أن يقتصر الوصول إلى أداة منع فقدان البيانات على الموظفين المصرح لهم، باستخدام ضوابط الوصول المادي والمنطقي وفقًا لسياسة الأمن المادي المعتمدة وسياسة إدارة هويات الدخول والصلاحيات الخاصة بـ<اسم الجهة>.
3-2	تعيين مسؤول أداة منع فقدان البيانات وفقًا للسياسات ذات الصلة المعتمدة لدى <اسم الجهة>.
3	ضبط إعدادات أداة منع فقدان البيانات (DLP tool configuration)
الهدف	ضبط إعدادات أداة منع فقدان البيانات لمراقبة وضبط حركة البيانات والمعلومات المدرجة في سجل منع فقدان البيانات.
المخاطر المحتملة	قد يؤدي ضبط الإعدادات بشكل غير صحيح لأداة منع فقدان البيانات والمعلومات إلى تسرب البيانات والمعلومات من خارج <اسم الجهة>
الإجراءات المطلوبة	
1-3	ضبط إعدادات أداة منع فقدان البيانات لتحديد جميع البيانات والمعلومات المدرجة في سجل منع فقدان البيانات، حيثما كان ذلك ممكنًا من الناحية الفنية.
2-3	ضبط إعدادات أداة منع فقدان البيانات لمراقبة وضبط حركة البيانات المدرجة في سجل منع فقدان البيانات باستخدام السياسات الفنية لمعالجة منع فقدان البيانات، مع تحديد مجموعة من قواعد أدوات الحماية من فقدان البيانات، بما في ذلك: أ) تحديد البيانات التي لا يمكن إرسالها أو نشرها أو تحميلها أو نقلها أو نسخها أو لصقها. ب) تحديد مكان نقل البيانات. ج) طريقة مشاركة البيانات.
3-3	ضبط إعدادات أداة منع فقدان البيانات لمسح متجهات فقدان البيانات المعروفة.
4-3	ضبط إعدادات أداة منع فقدان البيانات لاستخدام أداة أو أكثر من تقنيات الكشف التالية: أ) مطابقة المحتوى ب) الفهرسة أو بصمات الأصابع ج) التعرف الاختياري على الشخصية د) تقنيات الكشف الأخرى التي توفرها الأداة

5-3	ضـــبط إعدادات أداة منع فقدان البيانات لتطبيق قواعد أدوات منع فقدان البيانات من خلال واحدة أو أكثر من الآليات التالية: أ) حجب نقل البيانات والمعلومات المدرجة في سجل منع فقدان البيانات ب) رسائل الحجر الصحي قبل الإرسال ج) حجب النسخ واللصق على أجهزة التخزين الخارجية د) تسجيل جميع المخالفات
6-3	ضـــبط إعدادات أداة منع فقدان البيانات لتوفير التنبيهات للموظفين المصـــرح لهم عند حدوث خرق لقواعد أداة منع فقدان البيانات.
7-3	أن تكون الردود على التنبيهات الواردة من أداة منع فقدان البيانات خلال إطار زمني متفق عليه.
8-3	ضـــبط إعدادات أداة منع فقدان البيانات لإبلاغ المســـتخدمين بخرق قواعد أدوات منع فقدان البيانات.
9-3	مراجعة إعدادات أداة منع فقدان البيانات مرة واحدة على الأقل كل ستة أشهر.
10-3	يجب تحديث أداة منع فقدان البيانات عند الضـــرورة لتعكس التغييرات المحددة في المراجعة.
11-3	دمج أداة منع فقدان البيانات حيثما أمكن مع أداة إدارة المعلومات والأحداث الأمنية.
4	تسجيل منع فقدان البيانات DLP Logging
الهدف	جمع المعلومات حول أداء أداة منع فقدان البيانات وضمان عملها على النحو المطلوب.
المخاطر المحتملة	قد يؤدي عدم التسجيل إلى ضعف فهم أداء أداة منع فقدان البيانات، وما إذا كانت الأداة تعمل على النحو المطلوب أو المتوقع والافتقار إلى البيانات لأغراض ضـــمان الجودة والتدقيق.
الإجراءات المطلوبة	
1-4	أن تسجل أداة منع فقدان البيانات جميع الإجراءات والأنشطة.

2-4	تخزين سجلات أدوات منع فقدان البيانات في مكان آمن، على أن يقتصر الوصول إليها على الموظفين المصرح لهم، باستخدام ضوابط الوصول المادية والمنطقية.
3-4	الاحتفاظ بسجلات أدوات منع فقدان البيانات وفقًا لمتطلبات الاحتفاظ بما يتوافق مع السياسات ذات الصلة المعتمدة من قبل <اسم الجهة>.
4-4	حماية وسلامة سجلات أدوات منع فقدان البيانات (مثل: باستخدام التشفير أو الطوابع الزمنية الرقمية أو طرق أخرى يمكن إثبات التلاعب بها لحماية السلامة).
5-4	مراجعة السجلات الصادرة عن أداة منع فقدان البيانات وتحليلها مرة واحدة شهريًا على الأقل.
6-4	استخدام المعلومات من سجلات أداة منع فقدان البيانات عند الضرورة لتحسين أداء الأداة، وتقديم دليل على فقدان البيانات والمعلومات، وتقديم دليل على النجاح في إيقاف فقدان البيانات والمعلومات، أو لتسليط الضوء على متجهات جديدة لفقدان البيانات والمعلومات.
5	منع فقدان بيانات الأصول المعلوماتية (Information Asset Data Loss Prevention)
الهدف	تقليل احتمالية فقدان البيانات والمعلومات ذات الصيغة المادية.
المخاطر المحتملة	يمكن أن يؤدي فقدان المعلومات ذات الصيغة المادية إلى اختراقها أو انتهاكها أمنيًا، مما يؤدي إلى الإضرار بسمعة الجهة، وربما الخضوع إلى التحقيقات والغرامات القانونية والتنظيمية وذلك اعتمادًا على أصول المعلومات المفقودة.
الإجراءات المطلوبة	
1-5	يُحظر على الأفراد إزالة أصول المعلومات ذات الصيغة المادية (الأوراق والنسخ المطبوعة والعقود وما إلى ذلك) والمصنفة على أنها "مقيدة" أو تصنيف أعلى من ذلك من مقرات <اسم الجهة>.
2-5	يُحظر على الأفراد إزالة المعلومات المصنفة ذات الصيغة المادية (الأوراق والنسخ المطبوعة والعقود وما إلى ذلك) التي تعتبر بيانات شخصية من مقرات <اسم الجهة>.

الأدوار والمسؤوليات

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

2- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

3- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات>.

4- **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا على الأقل أو في حال حدوث تغييرات تقنية جوهرية في البنية التحتية أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالمعيار

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

2- يجب على جميع العاملين في <اسم الجهة> الالتزام بهذا المعيار.

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