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 إدارة الأصول

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 هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية ذات العلاقة بإدارة الأصول لأنظمة وبيانات ومعلومات الأصول الخاصة ب<اسم الجهة> وذلك لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية 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

ينطبق هذا المعيار على جميع الأصول المعلوماتية الخاصة ب<اسم الجهة> (مثل الأصول المادية والبيانات وتطبيقات الأعمال والبرمجيات والتقنيات)، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

1	قائمة جرد الأصول (Asset inventory)
الهدف	إنشاء (والحفاظ) على مخزون آمن من أصول المعلومات والتقنيات التي تمتلكها وتديرها <اسم الجهة> التي يمكن أن تعد قائمة جرد لكل نوع من أنواع الأصول على النحو المحدد في سياسة إدارة الأصول.
المخاطر المحتملة	في حال لم تمتلك <اسم الجهة> أو تحدث قائمة جرد الأصول، ستعاني الجهة من الأمور التالية: • عدم توافر تصور شامل بشأن الأصول التي تمتلكها وتديرها الجهة • صعوبة في تحديد مواقع الأصول • عدم القدرة على ضمان تحديث الأصول والحفاظ عليها حسب الاقتضاء • عدم التأكد من وجود ترتيبات الترخيص أو الاستخدام الصحيح المعمول به • عدم القدرة على حماية جميع الأصول من التهديدات السيبرانية
الإجراءات المطلوبة	
1-1	حفظ قائمة جرد الأصول في موقع آمن.
2-1	حماية قائمة جرد الأصول بضوابط الوصول المنطقية (مثل تلك المحددة في سياسة إدارة هويات الدخول والصلاحيات في <اسم الجهة>).

3-1	حماية قائمة جرد الأصول من التغييرات غير المصرح بها من خلال تقييد الوصول لهذه القائمة على الأفراد المصرح لهم.
4-1	عمل نسخ احتياطية لقائمة جرد الأصول بشكل منتظم وحمايته وفقًا لسياسة ومعيار النسخ الاحتياطي والاسترجاع في <اسم الجهة>.
5-1	الحرص على تحديث قائمة جرد الأصول بانتظام، من خلال إضافة الأصول عند امتلاكها أو شرائها وبعد نشرها أو التخلص منها.
6-1	التحقق من المعلومات المسجلة في قائمة جرد الأصول مرة واحدة سنويًا على الأقل للتأكد من دقتها لضمان استكمال تلك المعلومات وشموليتها وصحتها ودقة توقيتها.
2	محتويات قائمة جرد الأصول: أصول المعلومات الحساسة والمهمة (Asset (inventory contents: critical and sensitive information assets
الهدف	تسجيل المعلومات المهمة والحساسة التي تمتلكها <اسم الجهة>.
المخاطر المحتملة	يؤدي عدم وجود قائمة جرد للمعلومات المهمة والحساسة أو وجودها، ولكن بشكل غير كامل، إلى إضعاف قدرة <اسم الجهة> على فهم ما يلي: • الأصول الواجب حمايتها • مواقع تخزينها • الالتزامات التشريعية والتنظيمية للسياسات المرتبطة بالمعلومات الحرجة والحساسة • كيفية حماية المعلومات الحرجة والحساسة والتعامل معها.
الإجراءات المطلوبة	
1-2	تسجيل المعلومات التالية في قائمة جرد الأصول لكل أصل من أصول المعلومات الحرجة والحساسة (مثل عقد الاندماج والاستحواذ أو تفاصيل الراتب أو توقعات التسويق): أ) نوع المعلومات المصنفة ب) مستوى تصنيف المعلومات على النحو المحدد في سياسة تصنيف البيانات في <اسم الجهة> ج) تاريخ إعادة التصنيف د) متطلبات الالتزام (مثل تسجيل ما إذا كانت الأصول تندرج ضمن نطاق الخصوصية أو الاحتفاظ بالبيانات أو أي التزام قانوني آخر) ه) الأنظمة أو التطبيقات أو العمليات التي تعتمد على المعلومات من أجل التشغيل بشكل صحيح و) تحديد مالك المعلوماتية ز) موقع الأصول

	ح) مالك الأصول (مثل القائم على حماية الأصول)
3	الأصول المادية (Physical assets)
الهدف	تسجيل الأصول المادية التي تمتلكها وتديرها <اسم الجهة>.
المخاطر المحتملة	يؤدي عدم وجود قائمة جرد للأصول المادية إلى إضعاف قدرة <اسم الجهة> على فهم: • الأصول الواجب حمايتها • متطلبات الصيانة والترخيص والحماية.
الإجراءات المطلوبة	
1-3	جمع المعلومات التالية (شبكات، وتقنية المعلومات، والمعدات المتخصصة) وحفظها في قائمة جرد الأصول المادية: أ) نوع الأصول (مثل الشبكات وتقنيات المعلومات والمعدات المتخصصة) ب) وصف الأصول (مثل جدار الحماية أو الخادم أو الحاسوب الشخصي) ج) الشركة المصنعة للأصول وطرازها د) الغرض من الأعمال و/أو العمليات التجارية التي تدعمها الأصول ه) مالك الأصول (مثل الشخص المسؤول عن الأصل) ووحدة الأعمال المعنية و) الوصف أو المعرف المميز (مثل استخدام الأرقام التسلسلية أو عناوين الشبكة أو أرقام المنتجات) ز) التطبيقات التي تدعمها الأصول المادية ح) الموقع المادي ط) مستوى الحساسية لـ <اسم الجهة> أو التصنيف الممنوح للأصل ي) متطلبات الامتثال (مثل الأصل يندرج ضمن نطاق الهيئة الوطنية للأمن السيبراني أو جهة تنظيمية أخرى) ك) الأنظمة أو التطبيقات أو العمليات التي تعتمد على الأصل المادي للتشغيل السليم
2-3	يجوز إضافة المعلومات التالية في قائمة جرد الأصول، على الرغم من أن ذلك ليس إلزاميًا: أ) عناوين الأجهزة المرتبطة (على سبيل المثال عنوان التحكم بالوصول إلى الوسائط MAC address) ب) عناوين الشبكات المرتبطة (على سبيل المثال عناوين بروتوكول الإنترنت IP) ج) تفاصيل أي برمجيات مثبتة د) تفاصيل المنافذ النشطة أو الخدمات أو البروتوكولات على الأجهزة ه) تحديد ما إذا كانت الأجهزة معتمدة للاتصال بالشبكة و) حالة الاتصال الحالية (مثل: هل المعدات متصلة حاليًا بشبكات الجهة) ز) نتائج اختبار الأمن السيبراني

4	تطبيقات وبرمجيات الأعمال (Business applications and software)
الهدف	تسجيل تطبيقات الأعمال والبرامج المستخدمة من قِبل <اسم الجهة>.
المخاطر المحتملة	يؤدي عدم وجود أو عدم اكتمال قائمة جرد تطبيقات الأعمال وأصول البرمجيات إلى إضعاف قدرة <اسم الجهة> على فهم ما يلي: • الأصول الواجب حمايتها • متطلبات الصيانة والترخيص والحماية.
الإجراءات المطلوبة	
1-4	تسجيل المعلومات التالية الخاصة بتطبيقات الأعمال في قائمة جرد الأصول: أ) اسم تطبيق الأعمال ب) رقم نسخة التطبيق ج) مستوى التحديثات والإصلاحات د) نوع التطبيق مثل إدارة علاقات العملاء ومنصات التعاون ه) الغرض من الأعمال و/أو العمليات التجارية التي تدعمها الأصول و) مالك الأصول (مثل الشخص المسؤول عن الأصل) ووحدة الأعمال المعنية ز) المعلومات التي يعالجها كل تطبيق، مثل بيانات المعاملات المالية أو معلومات الأعمال الحساسة أو المعلومات المحددة للهوية الشخصية ح) التفاصيل الفنية حول كل تطبيق (مثل: متطلبات المورد والترخيص) ط) نتائج اختبار الأمن السيبراني ي) جهة الاتصال الخاصة بدعم الموردين
2-4	تسجيل المعلومات التالية في قائمة جرد الأصول الخاصة بالبرمجيات: أ) اسم البرنامج ب) رقم نسخة البرنامج ج) مستوى تحديثات وإصلاحات البرنامج د) نوع البرنامج (مثل: نظام التشغيل، برنامج الإنتاجية) ه) الغرض من الأعمال و/أو العمليات التجارية التي تدعمها الأصول و) مالك الأصول (مثل الشخص المسؤول عن البرنامج) ووحدة الأعمال المعنية ز) التفاصيل الفنية حول البرنامج (مثل: متطلبات المورد والترخيص) ح) نتائج اختبار الأمن السيبراني ط) جهة الاتصال الخاصة بدعم الموردين

5	الأطراف الخارجية والموردون (Third parties and suppliers)
الهدف	تسجيل الأطراف الخارجية والموردين الذين يقدمون السلع والخدمات لـ <اسم الجهة>.
المخاطر المحتملة	يؤدي عدم وجود أو عدم اكتمال قائمة الأطراف الخارجية والموردين إلى إضعاف قدرة <اسم الجهة> على فهم ما يلي: • السلع والخدمات المقدمة • المعلومات المتبادلة أو المشتركة أو المعالجة أو المنقولة أو المخزنة مع أطراف خارجية وموردين • المعلومات والأصول المادية التي يجب حمايتها في <اسم الجهة> والأطراف الخارجية والموردين.
الإجراءات المطلوبة	
1-5	بالنسبة للأطراف الخارجية والموردين، يجب ان تحتوي قائمة جرد الأصول على المعلومات التالية: أ) معرّف مميز ب) اسم الطرف الخارجي أو المورد ج) الغرض من الأعمال و/أو العمليات التجارية التي تدعمها الأصول د) مالك الأصول (مثل الشخص المسؤول عن الطرف الخارجي أو المورد) ووحدة الأعمال المعنية ه) عقد مبرم بين <اسم الجهة> والطرف الخارجي أو المورد و) أنواع السلع أو الخدمات المقدمة ز) أهمية السلع أو الخدمات المقدمة إلى <اسم الجهة> وعملياتها ح) جهة (جهات) الاتصال الخاصة بالأطراف الخارجية أو الموردين
2-5	يجب أن يكون لكل عقد مع طرف خارجي أو مورد قيد خاص ومُعرف فريد
3-5	بالنسبة للأطراف الخارجية والموردين، يجب ان تحتوي قائمة جرد الأصول على تفاصيل جميع الأجهزة والبرمجيات المقدمة من الجهة إلى أطراف خارجية في إطار العقد يجب أن تحتوي القائمة على المعلومات المطلوبة في قائمة جرد الأجهزة أو البرامج ذات الصلة
6	التحديث والمراجعة (Update and review)
الهدف	مراجعة قائمة جرد الأصول بشكل منتظم والتأكد من تحديثها

المخاطر المحتملة	يؤدي عدم تحديث قائمة جرد الأصول إلى توفير معلومات غير صحيحة عن الأصول لـ <اسم الجهة>، وعدم إجراء الترقيات اللازمة، وعدم القدرة على تحديد متطلبات الصيانة ومتطلبات الترخيص وحالة الأمن السيبراني.
الإجراءات المطلوبة	
1-6	تحديث قائمة جرد الأصول عن طريق إضافة الأصول عند شرائها وقبل نشرها
2-6	التحقق من المعلومات المسجلة في قائمة جرد الأصول مرة واحدة سنويًا على الأقل لضمان دقتها وللتأكد من استكمالها وشموليتها وصحتها ودقة توقيتها
3-6	مراجعة قائمة جرد الأصول من قبل جهة مستقلة على الأقل كل سنتين. ويجوز أن تتم هذه المراجعة في إطار أعمال التدقيق السنوي للأعمال أو التدقيق المالي
7	التخلص الآمن (Secure disposal)
الهدف	التخلص من معدات تقنية المعلومات والمعلومات الحساسة ذات الصيغ الرقمية والمادية بطريقة آمنة.
المخاطر المحتملة	يمكن الكشف عن المعلومات الحساسة والأسرار التجارية والبرمجيات والخوارزميات المخصصة عندما تتم إزالة المعدات والوثائق والسجلات الورقية مثل التقارير والتصاميم والدراسات التحليلية بشكل غير صحيح. وقد يؤدي هذا التعرض إلى فرض غرامات تنظيمية، وفقدان السمعة، والضرر التجاري، وفقدان الثقة من الحكومات والعملاء والأفراد.
الإجراءات المطلوبة	
1-7	حذف وسائط تخزين البيانات (بما في ذلك محركات الأقراص وأجهزة وسائط التخزين "USB" القابلة للإزالة) من جميع أصول تقنية المعلومات قبل التخلص منها.
2-7	إتلاف السجلات الورقية بشكل آمن باستخدام آلة تقطيع الورق وفقًا لمعيار المعهد الألماني للتوحيد القياسي (DIN) رقم 66399 وتحديدًا وفق البند P-3 أو أعلى
3-7	إتلاف السجلات الورقية المصنفة على أنها "سرية للغاية" و "سرية" بشكل آمن باستخدام آلة تمزيق الورق وفقًا لمعيار المعهد الألماني للتوحيد القياسي (DIN) وتحديد البند P-5 أو P-6 أو بالحرق.
4-7	إزالة جميع العلامات التعريفية، مثل بطاقات الأصول، من أي أصل من أصول تقنية المعلومات التي سيتم التبرع بها أو بيعها أو إعادتها إلى مؤسسة تأجير.

5-7	إتلاف جميع أصول الوسائط المادية والأجهزة التي تحتوي على بيانات مصنفة بطريقة آمنة تضمن استحالة استرداد البيانات.
6-7	يجوز لـ <اسم الجهة> التعاقد مع مورد معتمد لإتلاف المعلومات لتنفيذ عملية الاتلاف الآمن.
7-7	إصدار شهادات الإتلاف من قبل مورد خدمات الإتلاف للتأكيد على تنفيذ عملية الاتلاف الآمن.
8-7	تحديث قائمة جرد الأصول بالمعلومات ذات العلاقة بشأن التخلص من الأصول.
9-7	إنشاء سجل للإتلاف يتضمن جميع المعلومات اللازمة حول أنشطة الإتلاف مثل: أ) تاريخ عملية الإتلاف. ب) الأصول المتلفة. ج) نوع الأصول. د) الكمية. ه) الرمز أو رقم تعريف الأصل. و) التصنيف. ز) مشرف عملية الاتلاف. ح) طريقة الإتلاف. ط) شهادة إتلاف إذا قام بها المورد.

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>.