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 تصنيف الأصول

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.

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

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية ذات العلاقة بتصنيف الأصول الخاصة بأنظمة وبيانات ومعلومات <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

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

المعايير

١	تصنيف الأصول (Asset classification)
الهدف	تصنيف جميع الأصول التي تمتلكها وتديرها <اسم الجهة>.
المخاطر المحتملة	يؤدي عدم إعداد وتطبيق تصنيف الأصول في <اسم الجهة> إلى فشل في حماية الأصول باستخدام تدابير أو ضوابط وقائية غير مناسبة أو التعامل مع الأصول الحساسة بشكل غير صحيح، مما قد يؤدي إلى اختراقها أو تعرضها لانتهاكات أمنية.
الإجراءات المطلوبة	
١-١	يجب على <اسم الجهة> القيام بتصنيف جميع الأصول التي تمتلكها وتديرها.
١-٢	يجب تصنيف الأصول المادية (مثل أجهزة الاتصال بالشبكة، وأنظمة كشف التسلل ومنع التسلل (IDS/IPS)، وأصول التخزين، والأجهزة الطرفية للأنظمة الحساسة) بالرجوع إلى أعلى تصنيف لمدخلات المعلومات أو معالجتها أو تخزينها أو نقلها على الأصول المادية.

١-٣	يجب تصنيف تطبيقات الأعمال وأصول البرمجيات بالرجوع إلى أعلى تصنيف لمدخلات المعلومات، والتي تتم معالجتها أو تخزينها أو نقلها أو حذفها من قبل مستخدمي التطبيق أو البرنامج.
١-٤	يجب تصنيف الأطراف الخارجية والموردين بالرجوع إلى أعلى تصنيف لمدخلات المعلومات، أو معالجتها أو تخزينها أو نقلها أو حذفها من قبل الطرف الخارجي أو المورد.
١-٥	يجب تصنيف أي أصل (معلومات، وأصول مادية، وتطبيقات أعمال، وبرمجيات، وطرف خارجي ومورد) يعمل على إدخال أو معالجة أو حفظ أو نقل أو حذف المعلومات الشخصية و/أو الحساسة كـ "سري للغاية"، "سري"، "مقيد"، "عام" بالإضافة إلى أي تصنيف آخر مطلوب.
٢	ترميز الأصول المادية (Physical asset labelling)
الهدف	ترميز جميع الأصول المادية التي تمتلكها الجهة.
المخاطر المحتملة	يصعب تتبع أو مراقبة أو الرجوع إلى الأصول التي لم يتم ترميزها من قبل <اسم الجهة>، فالأصول التي لم يتم ترميزها قد لا يتم إدراجها في سجل الأصول، مما يؤدي إلى عدم تحديثها أو الحفاظ عليها بالشكل المناسب. وقد يتم التعامل مع الأصول المادية التي لم يتم ترميزها بشكل غير مناسب، مما قد يؤدي إلى تلفها أو سرقتها او فقدانها.
الإجراءات المطلوبة	
٢-١	يجب أن يكون لجميع الأصول المادية التي تمتلكها الجهة رموزًا مقاومة للتلاعب.
٢-٢	يجب أن تُظهر الرموز المقاومة للتلاعب رقمًا تعريفيًا مميزًا مخصصًا للأصل في سجل الأصول مثل الرقم أو الرمز الشريطي أو رمز الاستجابة السريع (QR).
٢-٣	يجب أن يحتوي الرمز المقاوم للتلاعب على رقم للاتصال.
٢-٤	يجب أن لا يحتوي الرمز المقاوم للتلاعب على اسم <اسم الجهة>، أو شعار <اسم الجهة>، أو أي علامات أو نصوص تعريفية أخرى.

٣	التعامل مع الأصول المادية (Physical asset handling)
الهدف	حماية الاصول من خلال التعامل معها بطريقة آمنة.
المخاطر المحتملة	يمكن أن يؤدي التعامل غير السليم أو الإهمال للأصول المادية إلى تلف أو فقدان أو سرقة الأصل وأي معلومات مخزنة أو متاحة على الجهاز. وبناءً على فئة أو نوع الأصول والمعلومات، قد تتعرض <اسم الجهة> إلى التحقيقات والغرامات القانونية أو التنظيمية.
الإجراءات المطلوبة	
٣-١	لا يجوز إزالة الأصول المادية (باستثناء الأصول المعتمدة كجزء من الأجهزة المحمولة) من مواقعها المخصصة.
٣-٢	يجب الحصول على الموافقة من مالك الأصل في حال إزالة الأصل المادي من موقعه المحدد.
٣-٣	يجب حذف وسائط التخزين مثل محركات الأقراص الصلبة المستخدمة لتخزين لمعلومات المصنفة مثل "سرية للغاية، و"سرية"، و"حساسة" باستخدام طرق الحذف المنشورة بحيث لا يتعذر استرجاع البيانات (مثلاً وفقًا لمعيار NIST SP800-88 Rev.1).
٣-٤	يجب إتلاف وسائط التخزين، مثل محركات الأقراص الثابتة، التي تم استخدامها لتخزين المعلومات المصنفة على أنها معلومات "سري للغاية" أو "سري" أو "مقيد"، إتلافًا ماديًا (على سبيل المثال عن طريق تمزيقها وفقًا لمعيار المعهد الألماني للتوحيد القياسي لا سيما البندين O-5 وH-5 أو حرقها).
٤	التعامل مع الأصول المادية للأجهزة المحمولة (Mobile device physical asset handling)
الهدف	حماية الأجهزة المحمولة من خلال التعامل معها بطريقة آمنة.
المخاطر المحتملة	يمكن أن يؤدي التعامل غير السليم للأصول المحمولة أو إهمالها إلى تلف أو فقدان أو سرقة الأصل وأي معلومات مخزنة أو متاحة على الجهاز. وبناءً على فئة ونوع الأصول والمعلومات، قد تتعرض <اسم الجهة> إلى التحقيقات والغرامات القانونية أو التنظيمية.
الإجراءات المطلوبة	

١-٤	يجب تدريب مستخدمي الأجهزة المحمولة مرة واحدة على الأقل في السنة على التعامل الآمن مع الأجهزة والبيانات (مثل أجهزة الحاسوب المحمولة والهواتف المحمولة وأجهزة التخزين المحمولة) التي يمكنها إدخال أو معالجة أو تخزين أو نقل أو حذف البيانات المصنفة. ويجب على المستخدمين الإقرار بحصولهم على الدورات التدريبية واستكمالها.
٢-٤	يجب إعادة الأجهزة المحمولة إلى موقع مركزي للتخلص منها.
٣-٤	يجب حذف وسائط التخزين، مثل محركات الأقراص الصلبة، في الأجهزة المحمولة التي تم استخدامها لتخزين المعلومات السرية المصنفة على أنها "سرية للغاية" أو "سرية" أو "حساسة" بشكل آمن باستخدام طريقة حذف آمنة بحيث يتعذر استرجاع البيانات بعد إيقاف تشغيلها (مثل: NIST SP800-88 Rev.1).
٤-٤	يجب إتلاف وسائط التخزين، مثل محركات الأقراص الصلبة، في الأجهزة المحمولة التي تم استخدامها لتخزين المعلومات السرية المصنفة على أنها "سرية للغاية" أو "سرية" أو "حساسة" بعد إيقاف تشغيلها (مثلاً عن طريق تمزيقها وفقًا للبند H-5 والبند O-5 من المعيار DIN 66399 أو حرقها).
٥-٤	يجب تحطيم أجهزة التخزين المحمولة التي أُستخدمت لتخزين المعلومات المصنفة بشكل مادي بعد إيقاف التشغيل (على سبيل المثال تمزيقها وفقًا للبند H-5 والبند O-5 من المعيار DIN 66399 أو حرقها).
٥	ترميز أصول المعلومات (Information asset labelling)
الهدف	ترميز الأصول المعلوماتية وتصنيفها.
المخاطر المحتملة	لن يتم التعامل مع أصول المعلومات التي لم يتم ترميزها بشكل صحيح، مما يزيد من احتمالية اختراقها أو تعرضها لانتهاكات أمنية.
الإجراءات المطلوبة	
١-٥	يجب ترميز أصول المعلومات المصنفة ذات الصيغة الرقمية (الملفات أو قواعد البيانات أو رسائل البريد الإلكتروني) إلكترونيًا (مثلاً من خلال استخدام الرؤوس والتذييلات في الوثائق أو تسمية الملفات أو التواقيع الرقمية).

٢-٥	يجب ترميز أصول المعلومات المصنفة ذات الصيغة المادية (الأوراق، والنسخ الورقية، والعقود، وما إلى ذلك) باستخدام آلية مقاومة للتلاعب مثل طوابع الحبر المطاطية والرموز اللاصقة والتصفيح ثلاثي الأبعاد.
٣-٥	يجب أن يكون للمعلومات التي تتم طباعتها على نسخة ورقية من خلال تطبيق أو برنامج أعمال رمز تصنيفي ذي صلة يتم وضعه قبل الطباعة (وفقًا لسياسة تصنيف البيانات المتبعة لدى <اسم الجهة>).
٦	التعامل مع أصول المعلومات (Information asset handling)
الهدف	التعامل مع أصول المعلومات بطريقة آمنة.
المخاطر المحتملة	قد يؤدي التعامل غير السليم لأصول المعلومات أو إهمالها وعدم الاكتراث بها إلى اختراقها أو تعرضها إلى انتهاكات أمنية. وبناءً على المعلومات التي تم انتهاكها أو اختراقها، قد تتعرض <اسم الجهة> للتحقيقات والعقوبات القانونية أو التنظيمية.
الإجراءات المطلوبة	
١-٦	يجب تشفير أصول المعلومات المصنفة ذات الصيغة الرقمية أثناء التخزين والنقل.
٢-٦	يجب إجراء عمليات نقل البيانات أو الملفات الإلكترونية باستخدام نظام معتمد وآمن لنقل الملفات (وليس البريد الإلكتروني أو تطبيقات المراسلة الأخرى).
٣-٦	يجب نقل البيانات أو الملفات التي تحتوي على معلومات سرية باستخدام وسائط اتصال آمنة، مثل البريد الإلكتروني عبر الشبكة الافتراضية الخاصة (VPN) أو بروتوكول نقل الملفات الآمن (SFTP).
٤-٦	يجب أن تتطلب أنظمة نقل الملفات استخدام خاصية مُعرف المستخدم، ويجب أن يسجل نظام نقل الملفات معرف المستخدم، والملفات المنقولة، والتاريخ والوقت على الأقل.
٥-٦	يجب مراجعة سجلات نظام نقل الملفات مرة واحدة شهريًا من قبل مالك تطبيق الأعمال.
٦-٦	يجب حماية أصول المعلومات المصنفة ذات الصيغة المادية (الأوراق العادية، والنسخ الورقية، والعقود، وما إلى ذلك) بوسائل مناسبة في جميع الأوقات، مثل حفظها بعيدًا في حالة عدم استخدامها ووضعها في المظاريف عند نقلها.
٧-٦	يجب حفظ أصول المعلومات المصنفة ذات الصيغة المادية في مكان آمن في نهاية كل يوم عمل، أو عند ترك المكتب دون مراقبة لأكثر من ساعة.

٦-٨	يمكن نقل أصول المعلومات ذات الصيغة المادية والمصنفة على أنها "حساسة" أو تصنيف أقل من مقرات <اسم الجهة> بطريقة آمنة (مثل: وضع الأوراق في ظرف مزدوج، مع ضمان عدم ورود أي معلومات تسهل التعرف على <اسم الجهة> بصورة ظاهرة، ووضع الأوراق في حقيبة أو حقيبة جهاز حاسوب محمول أو حقيبة أمتعة يدوية).
٦-٩	لا يجوز نقل أصول المعلومات ذات الصيغة المادية والمصنفة على أنها "حساسة" أو تصنيف أعلى من مقرات <اسم الجهة>.
٦-١٠	عند إرسال أصول المعلومات المصنفة ذات الصيغة المادية إلى أطراف خارجية أو موردين، يجب إرسالها بطريقة آمنة (مثل: وضع الأوراق في ظرف مزدوج، وضمان أن أي شيء يؤدي إلى التعرف على <اسم الجهة> لا يمكن رؤيته، ووضع الأوراق في طرد مضاد للعبث أو غير قابل العبث).
٦-١١	عند إرسال أصول المعلومات المصنفة ذات الصيغة المادية إلى أطراف خارجية أو موردين، يجب إرسالها باستخدام وسيلة المراسلة أو البريد الذي يمكن تتبعه. ويجب على المستلم التوقيع على إقرار بالاستلام.
٦-١٢	يجب إتلاف أصول المعلومات المصنفة ذات الصيغة المادية عن طريق تمزيقها، على سبيل المثال: باستخدام آلة تمزيق الورق بشكل متقاطع وفقًا للبند P-4 من معيار DIN 66399، أو أعلى (مثل P-5 أو P-6).
٦-١٣	لا يجوز نقل أصول المعلومات ذات الصيغة المادية والمصنفة على أنها "سرية للغاية" و"سرية" من مقرات <اسم الجهة>.
٦-١٤	يجب إتلاف أصول المعلومات ذات الصيغة المادية والمصنفة على أنها "سرية للغاية" أو "سرية" أو "حساسة" بشكل آمن عن طريق تمزيقها (مثلا: باستخدام آلة تمزيق الورق بشكل متقاطع وفقًا للبند P-5 أو البند P-6 من المعيار DIN 66399).

الأدوار والمسؤوليات

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

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

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

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

اختر التصنيف

الإصدار <١,٠>

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

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

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

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

الملحق

أ) مستويات تصنيف الأصول

مستوى التصنيف	الوصف
حساس	<يتم تصنيف الأصل على أنه "حساس"، إذا كان الوصول غير المصرح به أو إساءة الاستخدام يسببان آثارًا شديدة وواسعة على الجهة بطريقة يصعب حلها>
مرتفع	<يتم تصنيف الأصل على أنه "مرتفع"، إذا كان الوصول غير المصرح به أو إساءة الاستخدام يسبب آثارًا كبيرة على الجهة>
متوسط	<يتم تصنيف الأصل على أنه "متوسط"، إذا كان الوصول غير المصرح به أو إساءة الاستخدام يسبب آثارًا معتدلة على الجهة>
منخفض	<يتم تصنيف الأصل على أنه "منخفض"، إذا تسبب الوصول غير المصرح به أو سوء الاستخدام إلى آثار ضئيلة أو طفيفة على الجهة>

ب) مستويات تصنيف البيانات

مستوى التصنيف	الوصف
سري للغاية	<يتم تصنيف البيانات بتصنيف "سري للغاية"، إذا كان الوصول غير المصرح به أو إساءة الاستخدام يسببان آثارًا شديدة وواسعة على الجهة بطريقة يصعب حلها>

اختر التصنيف

الإصدار <١,٠>

سري	<يتم تصنيف البيانات بتصنيف "سري"، إذا كان الوصول غير المصرح به أو إساءة الاستخدام يسبب آثارًا كبيرة أو متوسطة على الجهة>
مقيد	<يتم تصنيف البيانات بتصنيف "متوسط"، إذا كان الوصول غير المصرح به أو إساءة الاستخدام يسبب آثارًا ضئيلة أو محدودة على الجهة>
عام	<يتم تصنيف البيانات بتصنيف "عام"، إذا كان الوصول غير المصرح به أو سوء الاستخدام لا يسبب أي آثار على الجهة>

اختر التصنيف

الإصدار <١,٠>