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 معيار الأمن المادي

اختر التصنيف

التاريخ	اضغط هنا لإضافة تاريخ
النسخة	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.

اختر التصنيف

الإصدار <1.0>

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

اختر التصنيف

الإصدار <1.0>

قائمة المحتويات

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية ذات العلاقة بالأمن المادي لمرافق ومباني وأصول <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 مرافق ومباني وأصول <اسم الجهة> في <على الجهة إضافة المواقع المادية حسب الحاجة مثل مراكز البيانات والمكاتب والمستودعات>)، وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

1	حماية المنشآت المادية (Physical Premises Protection)
الهدف	حماية المنشآت المادية من الضرر.
المخاطر المحتملة	يمكن أن تتعرض المنشآت والمباني والأصول المادية للسرقة أو التلف المادي، مما يؤدي إلى فقدان الأصول أو البيانات أو المعلومات أو انقطاع الخدمات التي تقدمها الأصول.
الإجراءات المطلوبة	
1-1	تحديد أدوار العاملين (بما في ذلك الموظفين والزوار والأفراد الآخرين) المسموح لهم بالوصول إلى المباني التي توجد فيها مراكز البيانات أو أجهزة الشبكة أو خوادم التطبيقات. ويشمل ذلك المباني التي تملكها أو تديرها <اسم الجهة> ووحدات الأعمال والأطراف الخارجية.
2-1	تحديد وتوثيق المواقع التي تتطلب ضوابط الوصول المادي، بما في ذلك جميع المناطق المصنفة على أنها حساسة، أو المناطق التي تحتوي على أنظمة أو بيانات مصنفة على أنها حساسة.
3-1	تحديد طرق الوصول إلى المنشآت والمرافق والمباني والأصول المادية الخاصة ب<اسم الجهة> في مستند عملية (process) ومراجعتها بشكل دوري.
4-1	تتضمن العملية الواردة في البند 1-3 المتطلبات التالية كحد أدنى:

اختر التصنيف

الإصدار <1.0>

	أ) يكون لدى العاملين الذين يطلبون الدخول إلى المباني والمنشآت عقد عمل ساري المفعول أو اتفاقية مقاول أو أمر عمل ب) كيفية تقديم طلب دخول إلى المنشآت والمباني (نموذج ورقي، بريد إلكتروني، نظام الطلبات، وغيرها) ج) الحاجة التي تستلزم الدخول إلى المنشآت والمباني د) الإطار الزمني أو الجدول الزمني أو الفترة الزمنية اللازمة للدخول ه) الشخص الذي يمكنه طلب الدخول (مثل: الموظفون في <اسم الجهة>) و) المسؤول عن التصريح بالدخول المطلوب ز) الوقت المطلوب للموافقة على طلب الدخول أو رفضه ح) تحديد الآلية التي سيتم استخدامها لمرافقة أو تتبع الدخول الفردي ط) كيفية تسجيل طلب الدخول بطريقة آمنة ي) كيفية تخزين طلبات الدخول المعتمدة، ومن ثم التحقق من وصول الأشخاص إلى موقع خاضع للرقابة ك) فترة صلاحية الدخول التي سيتم منحها
5-1	تسجيل جميع أحداث الدخول إلى المرافق والمباني والأصول المادية الخاصة بـ <اسم الجهة> فور حدوثها.
6-1	مراجعة صلاحيات الدخول مرة واحدة سنويًا على الأقل للتحقق من أن الدخول إلى المرافق والمباني والأصول المادية مناسب وساري المفعول.
7-1	إجراء مراجعة لتأكيد أو تغيير أو إلغاء الدخول مرة واحدة سنويًا على الأقل. ويمكن استخدام بيانات السجل التي جُمعت في هذه المراجعة.
8-1	إجراء مراجعة لتأكيد أو تغيير أو إلغاء الدخول إلى المواقع التي تستضيف الأنظمة الحساسة مرة واحدة على الأقل كل ستة أشهر. ويمكن استخدام بيانات السجل التي جُمعت في هذه المراجعة.
9-1	إلغاء تصاريح الدخول المادي غير النشطة بعد فترة زمنية متفق عليها بناءً على درجة حساسية النظام.
10-1	تسجيل الزوار الذين تم منحهم تصريحًا مؤقتًا بالدخول إلى المرافق والمباني والأصول المادية والإشراف عليهم شخصيًا من قبل العاملين المصرح لهم (بما في ذلك موظفي <اسم الجهة> من مواقع أو أقسام <اسم الجهة> الأخرى).
11-1	تطبيق ضوابط الدخول (مثل: استخدام الحواجز المادية، والأقفال، وقضبان النوافذ، والأبواب المعززة، وكاميرات المراقبة، والوصول المقيد إلى مراكز البيانات الموجودة في المباني الآمنة، واستخدام بطاقات الهوية من قبل جميع الزوار) للحد من الوصول إلى المرافق والمباني والأصول المادية الخاصة بـ <اسم الجهة>.

2	حماية البيئة (Environmental protection)
الهدف	توفير مرافق ومباني وأصول مادية بضمانات بيئية مناسبة.
المخاطر المحتملة	يمكن أن يتأثر تشغيل أنظمة تقنية المعلومات سلبًا بالبيئات الضارة أو غير الخاضعة للرقابة، مما يؤدي إلى ضعف في الأداء أو أخطاء أو إغلاق غير متوقع.
الإجراءات المطلوبة	
1-2	حماية المرافق والمباني والأصول المادية لـ <اسم الجهة> من خلال تطبيق متطلبات آلية الرقابة البيئية التالية كحد أدنى: أ) تكييف الهواء ب) التحكم في الرطوبة ج) نظام الكشف عن الحرائق د) أنظمة إخماد الحرائق المناسبة للبيئة.
2-2	استخدام نظام التزويد بالطاقة غير المنقطعة (UPS) أو ما شابهها لحماية أنظمة تقنية المعلومات الحساسة في حالة انقطاع التيار الكهربائي.
3-2	حماية الاتصالات وكابلات الطاقة، على سبيل المثال من خلال الحد من الوصول إلى غرف الاتصالات وغرف الشبكة، باستخدام قنوات الكابلات المحمية أو إخفاء مسارات الكابلات.
4-2	تحديد وتقييم مخاطر الكوارث الطبيعية وغير الطبيعية (من صنع الإنسان).
5-2	اختيار تدابير التخفيف وتنفيذها للحد من تأثير الكوارث الطبيعية والكوارث التي من صنع الإنسان (مثل: الحماية من الفيضانات وترتيبات استمرارية الأعمال وترتيبات الاعمال البديلة والمواقع البديلة) بالتنسيق مع <إدارة استمرارية الأعمال>.
3	التخلص الآمن (Secure disposal)
الهدف	ضمان التخلص من أصول تقنية المعلومات المادية وإتلافها بشكل آمن.
المخاطر المحتملة	قد يؤدي إتلاف أصول تقنية المعلومات والتخلص منها بطريقة غير آمنة إلى تعريض أي بيانات أو معلومات للمخاطر أو الاختراق، مما يؤدي إلى الإضرار بسمعة الجهة، وربما الخضوع إلى التحقيقات والعقوبات القانونية والتنظيمية وذلك اعتمادًا على البيانات أو المعلومات التي تم الإفصاح عنها.

الإجراءات المطلوبة	
1-3	تحديد الآليات واعتمادها من قبل <اسم الجهة> للتخلص من أصول تقنية المعلومات المادية بشكل آمن وفقًا لتصنيفها والمتطلبات التنظيمية ذات الصلة.
2-3	التخلص من جميع الأصول المادية التي وصلت إلى نهاية عمرها الافتراضي باستخدام الآليات المعتمدة الآمنة.
3-3	حماية النسخ المادية لوسائط النسخ الاحتياطي ووسائط التخزين لأصول تقنية المعلومات من الوصول أو الإتلاف أو التعديل غير المصرح به.
4-3	إنشاء سجل لدى <اسم الجهة> لتسجيل جميع أنشطة التخلص من الأصول المطبقة في المرافق والمباني والأصول المادية وحمايته من الوصول أو الإتلاف أو التعديل غير المصرح به.

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>.

اختر التصنيف

الإصدار <1.0>