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 الأمن السيبراني المتعلق بالأمن المادي

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 "<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 <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

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بحماية الأصول المادية الخاصة ب<اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية 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 العمل

تغطي هذه السياسة جميع المرافق والأصول المعلوماتية والتقنية والمعدات والأجهزة الخاصة ب<اسم الجهة> وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب حصر وتصنيف جميع الأصول المادية والمرافق الخاصة ب<اسم الجهة> وفقًا لسياسة تصنيف البيانات والمعلومات المعتمدة لدى <اسم الجهة>.

١-٢ يجب التحكم بالوصول للأماكن الحساسة مثل (مراكز البيانات، مراكز التعافي، أماكن معالجة المعلومات، مراكز المراقبة، غرف اتصالات الشبكة، مناطق الإمداد الخاصة بالأجهزة والمكونات التقنية) وتقييده للأشخاص المصرح لهم بذلك فقط.

١-٣ إعداد واعتماد وتطبيق الإجراءات التشغيلية اللازمة لمنح صلاحيات الوصول المادي لمرافق <اسم الجهة> استنادًا إلى مبادئ "الحاجة إلى المعرفة " و"الحاجة إلى الوصول" و"الحد الأدنى من الصلاحيات وعلى أن تتم مراجعتها وتدقيقها بشكل دوري.

١-٤ يجب استخدام أجهزة الكشف عن المعادن والمواد الخطيرة لعمليات الدخول للأماكن الحساسة في <اسم الجهة>.

١-٥ يجب تسجيل عمليات الدخول والخروج للأماكن الحساسة والاحتفاظ بالسجلات وحمايتها وفقًا لسياسة الأمن السيبراني لحماية البيانات المعتمدة لدى <اسم الجهة>.

١-٦ يجب مراقبة عمليات الدخول والخروج للأماكن الحساسة باستخدام تقنيات مثل (الدوائر التلفزيونية المغلقة "CCTV") وفقًا للمتطلبات والتشريعيات التنظيمية المعتمدة لدى <اسم الجهة> ومراقبتها من قبل عاملين مختصين بشكل مستمر.

١-٧ يجب تطوير إجراءات الاتلاف وإعادة الاستخدام والتخلص الآمن للأصول المادية التي تحتوي على معلومات مصنّفة وتشمل (الوثائق الورقية ووسائط التخزين والحفظ) مع الاحتفاظ بسجل للأصول التي تم إتلافها أو تمت إعادة استخدامها.

١-٨ يجب أن يتم التخلص من أجهزة البنية التحتية (Infrastructure Hardware)، وبالأخص معدات التخزين (Storage Equipment) بشكل آمن وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٩ يجب تطوير وتطبيق ومراجعة الضوابط الأمنية لحماية الأجهزة والمعدات داخل مباني <اسم الجهة> وخارجها بناءً على تصنيفها.

١-١٠ يجب تطوير وتطبيق إجراءات الاستجابة للطوارئ وخطط الإخلاء لمباني ومرافق <اسم الجهة> في حال الاشتباه أو وقوع أي حوادث مادية أو بيئية لضمان سلامة الموظفين وأصول <اسم الجهة> الحساسة.

١-١١ يجب مراجعة إجراءات وخطط الاستجابة للطوارئ دوريًا على أن يكون ذلك مرة واحدة على الأقل في السنة.

١-١٢ يجب تطوير وتطبيق إجراءات دعم وصيانة الأصول المادية والمعدات بما يتوافق مع المعايير الأمنية لصيانة المعدات المعتمدة لدى <اسم الجهة>.

١-١٣ يجب تقييم مخاطر الأمن السيبراني لرصد التهديدات الأمنية وتهديدات السلامة ومعرفة نقاط الضعف التي قد تواجهها <اسم الجهة> ومعالجتها لحماية الأصول المعلوماتية من التعرض لهذه التهديدات وفقًا لمنهجية إدارة المخاطر المعتمدة لدى <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١٤ يجب اختبار إمكانيات الأمن المادي وجاهزيته بشكل <سنوي>؛ من خلال عمل تمارين المحاكاة (مثل: الهندسة الاجتماعية).

١-١٥ يجب تقييد الحضور لاجتماعات <اسم الجهة> المصنفة على العاملين المصرح لهم فقط وتنفيذ المسح الأمني وتفتيش الحضور للاجتماعات المصنّفة.

١-١٦ يجب عدم منح الأطراف الخارجية صلاحية الوصول إلى المرافق الخاصة ب<اسم الجهة> إلا بعد تحقيق اشتراطات أمنية، على أن يتم مراقبة وصولهم ومرافقتهم في الأماكن التي تتطلب ذلك طوال مدة تواجدهم.

١-١٧ يجب تقييد صلاحية إدارة نظام الوصول المادي على أشخاص بامتيازات محددة ويتم تدقيقها ومراجعتها دوريًا وفقًا لسياسة إدارة هويات الدخول والصلاحيات المعتمدة لدى <اسم الجهة>..

١-١٨ يجب تأمين الوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية الخاصة بالأنظمة الحساسة ووسائطها، وحمايتها من الإتلاف، أو التعديل، أو الاطلاع غير المصرح به.

١-١٩ يجب تطبيق سياسة المكتب النظيف (Clear Desk Policy) والتأكد من عدم ترك أي وثائق أو أجهزة معلوماتية أو أجهزة التخزين الخارجية على مرأى من الأشخاص غير المصرح لهم.

١-٢٠ يجب على <الإدارة المعنية بالأمن السيبراني> التأكد من توفر الوعي الأمني اللازم لدى جميع العاملين حول أفضل الممارسات المتعلقة بالأمن المادي مثل المهمات والمسؤوليات المنوطة بهم وضمان التزامهم بها.

١-٢١ يجب إتلاف الأصول المادية التي تحوي معلومات مصنفة بشكل آمن.

اختر التصنيف

الإصدار <١,٠>

١-٢٢ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية الأمن المادي.

٢- ضوابط حماية الكابلات الصوتية والاتصالات والشبكة والطاقة ضد الأضرار المادية

يجب تنفيذ ضوابط لحماية الكابلات الصوتية والاتصالات والشبكة والطاقة ضد الأضرار المادية، بعد دراسة المخاطر المحتملة. كما يجب أن تغطي هذه الضوابط بحد أدنى ما يلي:

١-٢ حماية كابلات الاتصالات وشبكة البيانات من زراعه أجهزه تنصت (Wiretapping).

٢-٢ عدم تمديد كابلات الاتصالات وشبكة البيانات في مناطق تمكن أطراف خارجية من الوصول إليها.

٣-٢ حماية وعزل كابلات الاتصالات وشبكة البيانات بطريقة آمنة لحمياتها من الضرر أو الاعتراض غير المصرح به، وضمان تمديدها عبر مناطق آمنة ومحمية.

٤-٢ عزل كابلات الكهرباء والطاقة عن كابلات الاتصالات وشبكة البيانات.

٥-٢ استخدام مصادر طاقة متعددة وغير منقطعة مثل (Uninterruptible Power Source "UPS") لدعم التشغيل المستمر للأنظمة والأماكن الحساسة (مثل مراكز البيانات).

الأدوار والمسؤوليات

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

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

٣- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بالأمن المادي>.

٤- **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 السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالسياسة

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

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

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

اختر التصنيف

الإصدار <١,٠>