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

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

1. اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
2. أضف "<اسم الجهة>" في مربع البحث عن النص.
3. أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
4. اضغط على "المزيد" وتأكّد من اختيار "Match case".
5. اضغط على "استبدل الكل".
6. أغلق مربع الحوار.

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل الاسم الكامل للشخص>	اضغط هنا لإضافة نص	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدّل بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالأمن المادي في <اسم الجهة> تطبق بفعالية.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٤-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني. حيث يلزم الجهات حماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرّح به والفقدان والسرقة والتخريب، وبما يحقق سلامة وتوافر وحماية بيانات ومعلومات الفعالية.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة والأصول المعلوماتية والمعدات والأجهزة الخاصة بـ<اسم الجهة> وتنطبق على جميع العاملين في <اسم الجهة>.

بنود السياسة

1- يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرّح به، على أن تشمل بحد أدنى ما يلي:

1-1 التحكم بالوصول للأماكن الحساسة مثل (مراكز البيانات، مراكز التعافي، أماكن معالجة المعلومات، مراكز المراقبة، غرف اتصالات الشبكة، مناطق الإمداد الخاصة بالأجهزة والمكونات التقنية).

2-1 مراقبة ومراجعة سجلات الدخول والخروج مثل (الدوائر التلفزيونية المغلقة CCTV).

3-1 حماية السجلات ومصادر المعلومات من الوصول غير المصرّح به.

4-1 أمن واتلاف وإعادة استخدام الأصول المادية التي تحتوي على معلومات مصنّفة وتشمل (الوثائق الورقية ووسائط التخزين والحفظ).

5-1 أمن الأجهزة والمعدات داخل المباني وخارجها.

6-1 تطوير وتطبيق إجراءات الاستجابة للطوارئ وخطط الإخلاء لمباني ومرافق الجهة في حال الاشتباه أو وقوع أي حوادث مادية أو بيئية.

7-1 منع دخول السوائل والمواد الخطرة للأماكن الحساسة.

8-1 التحكم بدرجة حرارة الأماكن الحساسة للحفاظ على كفاءة أداء الأنظمة.

9-1 منع دخول الأفراد غير المصرّح لهم دخول القاعات والغرف المصنّفة والحصول على تصريح مسبق استناداً على مبدأ "الحاجة إلى المعرفة " و "الحاجة إلى الوصول" و "الحد الأدنى من الصلاحيات".

10-1صيانة المعدات والأجهزة داخل المباني وخارجها بشكل دوري.

2- 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:

2-1 حماية كابلات الاتصالات وشبكة البيانات من زراعه أجهزه تنصت (Wiretapping).

2-2 عدم تمديد كابلات الاتصالات وشبكة البيانات في مناطق تمكن أطراف خارجية من الوصول إليها.

2-3 حماية وعزل كابلات الاتصالات وشبكة البيانات بكفاءة من الضرر أو الاعتراض غير المصرح به، وضمان تمديدها عبر مناطق آمنة ومحمية.

2-4 عزل كابلات الكهرباء والطاقة عن كابلات الاتصالات وشبكة البيانات.

2-5 استخدام مصادر طاقة متعددة وغير منقطعة لدعم التشغيل المستمر للأنظمة والمرافق الحساسة (مثل مراكز البيانات)

3- تنفيذ تقييم لمخاطر الأمن المادي من قبل الجهات المسؤولة عن الأمن المادي عبر تحليل البيئة المادية والمناطق المحيطة لرصد التهديدات الأمنية وتهديدات السلامة ومعرفة مواطن الضعف ومعالجتها لحماية الأصول المعلوماتية من التعرض لهذه التهديدات.

4- على <الإدارة المعنية بالأمن المادي> تطوير واعتماد لائحة وإجراءات الأمن المادي والسلامة الخاصة بـ<اسم الجهة> أو بأي حدث أو فعالية تشارك في تنظيمها. بحيث تشمل تحديداً دقيقاً للواجبات، والمهام، لتكون بمثابة إطار عام لخدمة السلامة، والوقاية، والإنقاذ، ومكافحة الحريق، والإسعاف، ودليلاً مرشداً في سبيل حماية الأرواح والأصول والمعلومات.

5- تنفيذ المسح الأمني وتفتيش الحضور للاجتماعات المصنّفة، على أن يتم توفير أجهزة الكشف عن المعادن والمواد الخطيرة.

6- تصنيف جميع مرافق الجهة استناداً على تصنيف المعلومات التي يتم تداولها ومعالجتها فيها.

7- عدم منح الأطراف الخارجية صلاحية وصول مادي لمرافق الجهة إلا بعد تحقيق اشتراطات أمنية، على أن يتم مراقبة وصولهم ومرافقتهم في الأماكن التي تتطلب ذلك.

8- يجب أن تقتصر صلاحية إدارة نظام الوصول المادي على أشخاص بامتيازات محددة يمكن تدقيقها ومراجعتها.

9- مراجعة وتحديث صلاحيات الوصول المادي للمناطق الحساسة بشكل دوري.

10- توعية منسوبي الجهة حول أفضل الممارسات المتعلقة بالأمن المادي مثل سياسة المكتب النظيف وضمان التزامهم بها.

11- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني المتعلق بالأمن المادي.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

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

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

الالتزام بالسياسة

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذه السياسة دورياً.

2- يجب على جميع العاملين في <اسم الجهة> الالتزام بهذه السياسة.

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