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 أمن الشبكات

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

اختر التصنيف

الإصدار 1.0

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بأمن الشبكات الخاصة بـ<اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الشبكات التقنية الخاصة بـ<اسم الجهة> وتنطبق على جميع العاملين في <اسم الجهة>.

بنود السياسة

1- البنود العامة

1-1 تحديد وتوثيق جميع أجهزة الشبكة داخل <اسم الجهة> والتأكد من أن جميع الأجهزة محدثة ومعتمدة.

2-1 توثيق واعتماد معايير تقنية أمنية (Technical Security Standards) لجميع أجهزة الشبكة المستخدمة داخل <اسم الجهة>.

3-1 إدارة صلاحيات الدخول إلى الشبكات الخاصة بـ<اسم الجهة> وفقاً لسياسة إدارة هويات الدخول والصلاحيات، بحيث يكون الاتصال بالشبكة متوفراً عند الحاجة ومتاحاً للمستخدمين المصرح لهم فقط.

2- متطلبات الوصول إلى الشبكة

1-2 تطوير واعتماد إجراءات خاصة بمنح وإلغاء صلاحيات الدخول إلى الشبكة وذلك وفقاً لسياسة إدارة هويات الدخول والصلاحيات الخاصة بـ<اسم الجهة>.

2-2 للحصول على صلاحية الدخول إلى الشبكة، يجب على المستخدم تقديم طلب إلى <الإدارة المعنية بتقنية المعلومات> يوضح فيه نوع الطلب وفترة صلاحيته ومبرراته.

3-2 في حال إضافة أو التعديل على قوائم جدار الحماية، يجب على مسؤول الشبكة توثيق متطلبات الأعمال ومعلومات الطلب في نظام جدار الحماية.

4-2 يجب استخدام اسم المستخدم وكلمة المرور للدخول إلى الشبكة الخاصة بـ<اسم الجهة> وذلك وفقاً لسياسة إدارة هويات الدخول والصلاحيات.

5-2 مراجعة إعدادات وقوائم جدار الحماية (Firewall Rules) دورياً، وكل ستة أشهر على الأقل للأنظمة الحساسة. (CSCC-2-4-1-2)

6-2 توفير الحماية اللازمة عند تصفح الإنترنت والاتصال به، وتقييد الدخول إلى المواقع الإلكترونية المشبوهة، ومواقع مشاركة تخزين الملفات، ومواقع الدخول عن بعد.

7-2 عدم ربط الشبكة اللاسلكية بالشبكة الداخلية لـ<اسم الجهة>، إلا بناءً على دراسة متكاملة للمخاطر المترتبة على ذلك، والتعامل معها بما يضمن حماية الأصول التقنية الخاصة وسرية البيانات وسلامتها، وحماية النظم والتطبيقات المتصلة بـ<اسم الجهة>.

8-2 يُمنع ربط الأنظمة الحساسة بالشبكة اللاسلكية لـ<اسم الجهة>.

9-2 يجب توفير التقنيات اللازمة لوضع القيود وإدارة منافذ وبروتوكولات وخدمات الشبكة.

10-2 يمنع الربط المباشر لأي جهاز بالشبكة المحلية للأنظمة الحساسة قبل فحصه والتأكد من توافر عناصر الحماية المحققة للمستوى المقبول للأنظمة الحساسة (CSCC-2-4-1-3).

3- متطلبات وصول الأطراف الخارجية إلى الشبكة

1-3 يخضع منح صلاحية وصول الأطراف الخارجية إلى شبكة <اسم الجهة> لمتطلبات الأمن السيبراني المشار إليها في سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية.

2-3 استخدام تقنيات تشفير ومصادقة آمنة لنقل البيانات من الأطراف الخارجية وإليها.

3-3 تحديد مدة زمنية معينة للأطراف الخارجية للدخول إلى شبكة <اسم الجهة>.

4-3 مراجعة صلاحيات المستخدمين والأطراف الخارجية دورياً وذلك وفقًا لسياسات الأمن السيبراني المعتمدة في <اسم الجهة>.

4- حماية الشبكات

1-4 يجب عزل وتقسيم الشبكات مادياً ومنطقياً باستخدام جدار الحماية (Firewall) ومبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth). (ECC-2-5-3-1)

2-4 تطبيق العزل المنطقي لشبكة الأنظمة الحساسة (VLAN).

3-4 تطبيق العزل المنطقي بين شبكة بيئة الإنتاج وشبكة بيئة الاختبار والشبكات الأخرى.

4-4 يمنع ربط الأنظمة الحساسة بالإنترنت في حال كانت هذه الأنظمة تقدم خدمة داخلية لـ<اسم الجهة> ولا توجد هناك حاجة ضرورية جداً للدخول على الخدمة من خارج <اسم الجهة>. (CSCC-2-4-1-6)

5-4 تطبيق العزل المنطقي بين شبكة الاتصالات الهاتفية عبر الإنترنت (Voice Over IP "VOIP") وشبكة البيانات.

6-4 تقييد استخدام منافذ الشبكة المادية في جميع مرافق <اسم الجهة> وذلك باستخدام خاصية حماية المنافذ (Port Security) أو تقنية التحقق من الأجهزة (Port-Based Authentication) لحماية الشبكة من احتمالية ربط أجهزة غير مصرح بها أو أجهزة مشبوهة دون أن يتم كشفها.

7-4 توفير أنظمة الحماية في قناة تصفح الإنترنت للحماية من التهديدات المتقدمة المستمرة (APT Protection) التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المتوقعة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن.

4-8 يمنع اتصال الشبكة الداخلية بالإنترنت مباشرةً، ويكون الاتصال عن طريق استخدام موزع اتصالات الإنترنت (Proxy) لتحليل وتصفية البيانات المنتقلة من وإلى <اسم الجهة>.

4-9 ضبط إعدادات قوائم جدار الحماية بحيث تُحظر جميع أنواع الاتصالات بين أجزاء الشبكة تلقائياً (Explicitly)، ويتم إتاحة قوائم جدار الحماية بناءً على طلب المستخدم ومتطلبات الأعمال.

4-10 يجب توفير التقنيات اللازمة لأمن نظام أسماء النطاقات (DNS).

4-11 يجب توفير أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention Systems) على جميع أجزاء الشبكة وتحديثها دورياً.

4-12 يجب توفير أنظمة الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة (Network APT) على شبكة الأنظمة الحساسة.

4-13 يجب تطبيق آليات حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة (APT) والبرمجيات الضارة غير المعروفة مسبقاً وإدارتها بشكل آمن. (ECC-2-5-3-8)

4-14 يجب توفير أنظمة الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS") على الأنظمة الخارجية الحساسة. (CSCC-2-4-1-8)

5- الأمن المادي والبيئي

5-1 يجب حفظ أجهزة الشبكات في بيئة آمنة وملائمة، والتأكد من ضبط درجة الحرارة والرطوبة وكذلك وجود مصادر طاقة احتياطية مثل (Uninterruptible Power Supply "UPS").

5-2 يجب تقييد الدخول المادي إلى أجهزة الشبكات للمصرح لهم فقط لحفظ الأجهزة وحمايتها من السرقة أو العبث.

5-3 يجب حفظ سجلات الدخول ومراقبة مناطق أجهزة الشبكات الخاصة بالأنظمة الحساسة (CCTV) ومراجعتها دورياً.

6- متطلبات أخرى

6-1 يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لأمن الشبكات.

6-2 يجب مراجعة متطلبات الأمن السيبراني الخاصة بأمن الشبكات سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

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 بتقنية المعلومات> و<الإدارة المعنية بالأمن السيبراني>.

الالتزام بالسياسة

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

2- يجب على كافة 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>.