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

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 "<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 <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	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 <١,٠>

قائمة المحتويات

اختر التصنيف

الإصدار <١,٠>

الغرض

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المتعلقة بحماية الشبكات الخاصة ب<اسم الجهة> لتحقيق الغرض الأساسي من السياسة وهو تقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية في <اسم الجهة>. هذه المتطلبات تمت موائمتها مع متطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني ويشمل ذلك على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – ١: ٢٠١٨)، ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – ١: ٢٠١٩) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل

تطبق هذه السياسة على جميع الشبكات التقنية والأجهزة الشبكية الخاصة ب<اسم الجهة> وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب حصر جميع أجهزة الشبكة الخاصة ب<اسم الجهة> والتأكد من أن جميع الأجهزة محدثة ومعتمدة.

١-٢ يجب حصر واعتماد ومراجعة أفضل المعايير والممارسات التقنية الأمنية العالمية (Technical Security Standards) لجميع أجهزة الشبكة المستخدمة في <اسم الجهة>، وتطبيق مبدأ الدفاع الأمني متعدد المراحل على الشبكة (Defense-in-Depth).

١-٣ يجب إدارة صلاحيات الدخول إلى الشبكات الخاصة ب<اسم الجهة> وفقًا لسياسة إدارة هويات الدخول والصلاحيات، بحيث يكون الاتصال بالشبكة متوفرًا عند الحاجة ومتاحًا للمستخدمين المصرح لهم فقط.

١-٤ يجب تفعيل وتسجيل السجلات لجميع أجهزة وأنظمة <اسم الجهة> والاحتفاظ بها، وفقًا لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدة لدى <اسم الجهة>.

١-٥ يجب الاحتفاظ لمستندات التصاميم الخاصة بالشبكة وضمان تحديثها بشكل مستمر.

١-٦ يجب مزامنة توقيت جميع الخوادم مركزيًا (Clock Synchronization) ومن مصدر دقيق وموثوق ومعتمد.

١-٧ يجب تطبيق متطلبات جميع السياسات ذات العلاقة لأمن الشبكات المعتمدة لدى <اسم الجهة> على سبيل المثال لا الحصر السياسات التالية:

١-٧-١ سياسة أمن البريد الإلكتروني المعتمدة لدى <اسم الجهة> وفقًا للسياسات والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٧-٢ سياسة إدارة حزم التحديثات والإصلاحات المعتمدة لدى <اسم الجهة> وفقًا للسياسات والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٧-٣ سياسة حماية تطبيقات الويب المعتمدة لدى <اسم الجهة> وفقًا للسياسات والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٨ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات الأمن السيبراني لأمن الشبكات.

٢- متطلبات الوصول إلى الشبكة

٢-١ يجب تطوير واعتماد إجراءات خاصة بمنح وإلغاء صلاحيات الوصول إلى شبكات <اسم الجهة> وذلك وفقًا لسياسة إدارة هويات الدخول والصلاحيات الخاصة ب<اسم الجهة>.

٢-٢ للحصول على صلاحية الدخول إلى الشبكة، يجب على المستخدم تقديم طلب إلى <الإدارة المعنية بتقنية المعلومات> يوضح فيه نوع الطلب وفترة صلاحيته ومبرراته.

٢-٣ في حال الإضافة أو التعديل على قوائم جدار الحماية، يجب الحصول على الموافقات اللازمة وعلى مسؤول الشبكة توثيق متطلبات الأعمال ومعلومات الطلب في نظام جدار الحماية.

٢-٤ يجب استخدام اسم المستخدم وكلمة المرور للدخول إلى الشبكة الخاصة ب<اسم الجهة> وذلك وفقًا لسياسة إدارة هويات الدخول والصلاحيات المعتمدة لدى <اسم الجهة>.

٢-٥ يجب توفير التقنيات اللازمة لوضع القيود وإدارة منافذ وبروتوكولات وخدمات الشبكة.

٢-٦ يجب 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.

٢-٧ يجب تقييد منافذ وبروتوكولات وخدمات الشبكة المستخدمة لعمليات الدخول عن بعد، وخصوصًا على الأنظمة الداخلية والأنظمة الحساسة، وفتحها حسب الحاجة.

٣- متطلبات وصول الأطراف الخارجية إلى الشبكة

٣-١ يجب أن يخضع منح صلاحية وصول الأطراف الخارجية إلى شبكة <اسم الجهة> لمتطلبات الأمن السيبراني المشار إليها في سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية المعتمدة لدى <اسم الجهة>.

٣-٢ يجب استخدام تقنيات تشفير ومصادقة آمنة لنقل البيانات من الأطراف الخارجية وإليها.

٣-٣ يجب تحديد مدة زمنية معينة للأطراف الخارجية للدخول إلى شبكة <اسم الجهة> حسب ما يتم الاتفاق عليه مع مالك النظام.

٣-٤ يجب مراجعة صلاحيات المستخدمين والأطراف الخارجية دوريًا وذلك وفقًا لسياسات الأمن السيبراني المعتمدة في <اسم الجهة>.

٣-٥ يجب منع الوصول المباشر لخدمات التحقق، وإدارة الدخول عن بعد (Remote Access Management and Authentication) على الأجهزة المتواجدة في الشبكة الخارجية للجهة (External-Facing Host).

٦-٣ يجب منع الأشخاص التابعين لأطراف خارجية بالاتصال بالشبكة أو الشبكة اللاسلكية لـ<اسم الجهة> دون فحص للثغرات الأمنية وتحديث برنامج مكافحة الفيروسات وضبط الإعدادات المناسبة والتأكد من إمكانية مراقبة الأنشطة الخاصة بهم.

٤- حماية الشبكات

٤-١ يجب عزل وتقسيم الشبكات ماديًا ومنطقيًا باستخدام جدار الحماية (Firewall) ومبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth).

٤-٢ يجب تطبيق العزل المادي والمنطقي لشبكة الأنظمة الحساسة (VLAN).

٤-٣ يجب تطبيق العزل المنطقي والمادي بين شبكة بيئة الإنتاج وشبكة بيئة الاختبار والشبكات الأخرى.

٤-٤ يجب مراقبة الشبكات الداخلية والخارجية للكشف عن الأنشطة المشبوهة.

٤-٥ يجب منع ربط الأنظمة الحساسة بالإنترنت في حال كانت هذه الأنظمة تقدم خدمة داخلية لـ<اسم الجهة> ولا توجد هناك حاجة ضرورية جدًا للدخول على الخدمة من خارج <اسم الجهة>.

٤-٦ يجب تطبيق العزل المنطقي بين شبكة الاتصالات الهاتفية عبر الإنترنت (Voice Over IP "VOIP") وشبكة البيانات.

٤-٧ يجب استخدام التقنيات المناسبة لتأمين التصفح والاتصال بالإنترنت، ويشمل ذلك التقييد الحازم للمواقع الالكترونية المشبوهة، ومواقع مشاركة وتخزين الملفات، ومواقع الدخول عن بعد.

٤-٨ يجب اعتماد حزم التحديثات الدورية، والإصلاحات الأمنية للأصول في بيئة الإنتاج، من قبل الشركة المصنعة، وإجراء اختبار في بيئة تجريبية قبل تطبيقها على بيئة الإنتاج.

٤-٩ يجب توفير أنظمة الحماية في قناة تصفح الإنترنت للحماية من التهديدات المتقدمة المستمرة (APT Protection) التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المتوقعة مسبقًا (Zero-Day Malware)، وإدارتها بشكل آمن وتحديثها باستمرار.

٤-١٠ يجب منع اتصال الشبكة الداخلية بالإنترنت مباشرةً، ويكون الاتصال عن طريق استخدام موزع اتصالات الإنترنت (Proxy) لتحليل وتصفية البيانات المنتقلة من وإلى <اسم الجهة>.

٤-١١ يجب ضبط إعدادات قوائم جدار الحماية بحيث تُحظر جميع أنواع الاتصالات بين أجزاء الشبكة تلقائيًا (Explicitly)، ويتم إتاحة قوائم جدار الحماية بناءً على طلب المستخدم ومتطلبات الأعمال ومراجعتها دورياً.

٤-١٢ يجب توفير التقنيات اللازمة لتأمين نظام أسماء النطاقات (DNS).

٤-١٣ يجب توفير أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات مثل (Intrusion Prevention/Detection Systems (IDS/IPS,HIDS/HIPS) على جميع أجزاء الشبكة وتحديثها بشكل مستمر.

٤-١٤ يجب توفير أنظمة الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة (Network APT) على شبكة الأنظمة الحساسة وتحديثها بشكل مستمر.

٤-١٥ يجب توفير أنظمة الحماية من هجمات تعطيل الشبكات والخدمات (Distributed Denial of Service Attack "DDoS") على الأنظمة وتحديثها بشكل مستمر.

اختر التصنيف

الإصدار <١,٠>

٤-١٦ يجب استخدام التقنيات المناسبة لحماية القناة المستخدمة للاتصال الشبكي مع مقدم خدمة الحوسبة السحابية.

٤-١٧ يجب تقييد استخدام اتصالات الشبكة والخدمات ونقاط الاتصال بين المناطق المختلفة (Zones) وحصرها على الحد الأدنى لتلبية متطلبات التشغيل والصيانة والسلامة.

٤-١٨ يجب مراجعة إعدادات وقوائم جدار الحماية (Firewall Rules) سنويًا، وكل ستة أشهر على الأقل لجدار الحماية الخاص بشبكات الأنظمة الحساسة.

٤-١٩ يجب تطوير وتحديث قائمة (Blacklist) لعناوين بروتوكول الإنترنت والمواقع الإلكترونية الضارة المعروفة مسبقًا وحظرها.

٤-٢٠ يجب عدم ربط الشبكة اللاسلكية بالشبكة الداخلية لـ<اسم الجهة>، إلا بناءً على دراسة متكاملة للمخاطر المترتبة على ذلك، واستخدام وسائل آمنة للتحقق من الهوية والتشفير، والتعامل معها بما يضمن حماية الأصول التقنية الخاصة وسرية البيانات وسلامتها، وحماية النظم والتطبيقات المتصلة بـ<اسم الجهة>.

٤-٢١ يجب منع ربط الأنظمة الحساسة بالشبكة اللاسلكية لـ<اسم الجهة>.

٤-٢٢ يجب منع الربط المباشر لأي جهاز بالشبكة المحلية للأنظمة الحساسة إلا بعد فحصه والتأكد من توافر عناصر الحماية المحققة للمستوى المقبول للأنظمة الحساسة.

٤-٢٣ يجب تقييم واختبار الشبكة الداخلية والخارجية لـ<اسم الجهة> والتأكد من أن المخاطر الأمنية في الشبكة وفق مستوى المخاطر المقبول لدى <اسم الجهة> بشكل دوري، مرة واحدة كل سنة على الأقل.

٤-٢٤ يجب توفير التقنيات اللازمة لفك تشفيرحركة مرور الويب (SSL/HTTPS Inspection).

٤-٢٥ يجب تقييد الدخول والاتصال عن بعد للأنظمة الحساسة فقط عند الحاجة، توفير آليات وبروتوكولات وتقنيات حديثة وآمنة لضمان اتصال آمن مثل (VPN, Site-to-Site VPN).

٤-٢٦ السماح بقائمة محددة (Whitelisting) فقط، لقوائم جدار الحماية، الخاصة بالأنظمة الحساسة.

٥- الأمن المادي والبيئي

٥-١ يجب حفظ أجهزة الشبكات في بيئة آمنة وملائمة، والتأكد من ضبط درجة الحرارة والرطوبة وكذلك وجود مصادر طاقة احتياطية مثل (Uninterruptible Power Supply "UPS").

٥-٢ يجب تقييد الدخول المادي إلى أجهزة الشبكات للمصرح لهم فقط لحفظ الأجهزة وحمايتها من السرقة أو العبث.

٥-٣ يجب تسجيل عمليات الدخول وحفظ السجلات الخاصة بها ومراقبة مناطق أجهزة الشبكات باستخدام أنظمة المراقبة بالفيديو (CCTV) ومتابعتها بشكل مستمر.

الأدوار والمسؤوليات

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

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

٣- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بتقنية المعلومات> و<الإدارة المعنية بالأمن السيبراني>.

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 (الموظفين والمتعاقدين) 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>