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 معيار أمن الشبكات

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.

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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.

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

يهدف هذا المعيار إلى تحديد متطلبات الأمن السيبراني التفصيلية لحماية أمن الشبكات الخاصة ب<اسم الجهة> لتحقيق الغرض الأساسي وهو تقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية في <اسم الجهة>. هذه المتطلبات تمت موائمتها مع سياسة أمن الشبكات ومتطلبات 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.

النطاق

يطبق هذا المعيار على جميع أنظمة الشبكات التقنية الخاصة ب<اسم الجهة>، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعيار

١	الوصول الآمن
الهدف	ضمان تطبيق الإعدادات الأمنية الملائمة للوصول إلى واجهات إدارة أمن الشبكات من أجل حمايتها بشكل فعال من الهجمات السيبرانية.
المخاطر المحتملة	يؤدي ضعف الإعدادات لحلول واجهات إدارة أمن الشبكات إلى تعرض أجهزة الشبكات داخل بيئة <اسم الجهة> إلى هجمات أو انتهاكات أمنية.
الإجراءات المطلوبة	
١-١	تطبيق أفضل معايير الوصول الآمن للشبكات وفقًا للمعايير المذكورة في معيار إدارة هويات الدخول والصلاحيات المعتمد لدى <اسم الجهة>.
١-٢	إعداد قائمة وصول لحماية جميع أجزاء الشبكة من انتحال عنوان بروتوكول الإنترنت (from Layer-٣ IP address spoofing).
١-٣	تقييد وصول مشرفي إدارة مكونات الشبكة اللاسلكية عبر استخدام أجهزة حاسب مخصصة ذات الصلاحيات والامتيازات الهامة والحساسة (PAWs) أو خوادم الوصول إلى المناطق الآمنة (Jump Servers) الموجودة على واجهات إدارة مستقلة على شبكة مفصولة عن شبكة <اسم الجهة> ومعزولة عن الإنترنت، ومنع وصولهم لاسلكيًا.

٢	فصل الشبكة
الهدف	ضمان حماية تصميم وبنية الشبكة وحماية الأجزاء الشبكية وفقًا لمستوى الأمن الخاص بها من خلال الفصل بين أجزاء الشبكة.
المخاطر المحتملة	تتشارك الشبكات غير المفصولة في نفس نطاق البث وتكون الأجهزة قادرة على التواصل دون مراقبة أو ضبط حركة البيانات، وبالتالي يمكن أن يؤدي أي هجوم على النظام إلى تهديدات داخلية خطيرة وهجمات على معظم أنظمة الشبكة، مما يسهل حركة البيانات الجانبية ضمن الشبكة.
الإجراءات المطلوبة	
٢-١	تصميم وتطبيق شبكة معزولة منطقيًا و/أو ماديًا مع الأخذ بعين الاعتبار احتياجات الأعمال والمعمارية المؤسسية وذلك بالاستناد إلى الدفاع الأمني متعدد المراحل والمعمارية متعددة المستويات.
٢-٢	تطبيق المستوى الملائم من ضوابط الأمن السيبراني على الأجزاء الشبكية المختلفة بناءً على قيمة وتصنيف المعلومات المخزنة أو المعالجة في الشبكة ومستويات الموثوقية والتأثير على الأعمال والمخاطر المرافقة.
٢-٣	تطبيق المعمارية متعددة المستويات المحمية بجدار حماية ثنائي الطبقة. وعلى وجه الخصوص، تقسيم الشبكة إلى ثلاثة مستويات أو أكثر (مستوى الحدود/المحيط، والمستوى الرئيسي، والمستوى الموثوق)، وتقسيم الأجزاء الشبكية إلى مناطق (المنطقة المحايدة "DMZ"، ومنطقة الإدارة، ومنطقة الإنتاج، ومنطقة التطوير/الاختبار، وغيرها) وفقًا للبنية المؤسسية والبنية الأمنية في <اسم الجهة>.
٢-٤	تصميم وإعداد الشبكات لتصفية مرور البيانات بين مختلف أجزاء الشبكة ومنع الوصول غير المصرح به.
٢-٥	وضع الخوادم أو مخازن البيانات التي تتضمن معلومات حساسة في أجزاء شبكية منفصلة ومخصصة.
٢-٦	إعداد جدران الحماية والموجّهات (Routers) لمنع أي اتصالات غير مصرح بها بين الشبكات غير الموثوقة وأي مكونات نظام تقوم بتخزين معلومات حساسة.
٢-٧	تحديد وتطبيق المستويات والحدود لكل منطقة أمنية.
٢-٨	تحديد وتطبيق منطقة أو جزء شبكي لواجهات الإدارة المستقلة، بما في ذلك كافة خوادم الإدارة، والمعدات ذات صلاحية الوصول الإدارية، وخوادم بروتوكول النقل الآمن

	(SSH)، وخوادم الوصول إلى المناطق الآمنة (Jump Servers)، وأجهزة الحاسب ذات الصلاحيات والامتيازات الهامة والحساسة (PAWs).
٢-٩	فصل الشبكات اللاسلكية عن الشبكة الداخلية والشبكات المعزولة والشبكات الخاصة.
٢-١٠	تحديد الخوادم والشبكات وبيئات الإنتاج والاختبار والبيئات الحساسة المستخدمة في تطوير واختبار وفحص وتخزين البيانات والنشاطات ذات الصلة وفصلها عن الشبكات الأخرى.
٢-١١	فصل أجزاء الأنظمة الحساسة منطقيًا عن البيئات الأخرى.
٢-١٢	منع الأنظمة الحساسة من الاتصال بالشبكة اللاسلكية.
٢-١٣	منع الأنظمة الحساسة من الاتصال بالإنترنت في حال كانت هذه الأنظمة تقدم خدمات داخلية ولا تحتاج إلى صلاحية الوصول عن بعد أو الوصول عبر الإنترنت.
٢-١٤	مراجعة الإعدادات والقواعد والسياسات والملفات التعريفية الأمنية لجدران الحماية والموجهات (Routers) التي تدعم الشبكات الحساسة مرة كل ستة أشهر على الأقل.
٣	تأمين الحدود
الهدف	حماية حدود الشبكة من التهديدات السيبرانية.
المخاطر المحتملة	في حال لم يتم تطبيق الضوابط الأمنية الملائمة لحماية حدود الشبكة، قد يتمكن المهاجمون من اختراق الشبكة بسهولة وفرض المزيد من التهديدات الخطيرة.
الإجراءات المطلوبة	
٣-١	الاحتفاظ بقائمة جرد محدثة لكافة حدود الشبكة في <اسم الجهة>.
٣-٢	القيام بعمليات مسح وفحص منتظمة من الخارج لكل حد شبكة موثوق لاكتشاف أي اتصالات غير مصرح بها يمكن الوصول إليها عبر الحدود.
٣-٣	حظر الاتصالات مع عناوين بروتوكولات الإنترنت الضارة أو غير المستخدمة وحصر الوصول بمجالات عنوان بروتوكولات الإنترنت الموثوقة والضرورية عند كل حد من حدود شبكة <اسم الجهة>.
٣-٤	حظر الاتصالات عبر منافذ بروتوكول التحكم بالنقل (TCP) أو بروتوكول حزم بيانات المستخدم (UDP) أو حركة التطبيقات لضمان السماح فقط للبروتوكولات المصرح لها

	بالدخول أو الخروج من الشبكة عبر حدود الشبكة عند كل حد من حدود شبكة <اسم الجهة>.
٣-٥	إعداد أنظمة المراقبة لتسجيل حزم بيانات الشبكة التي تمر عبر الحدود عند كل حد من حدود شبكة <اسم الجهة>.
٣-٦	تثبيت حساسات أنظمة كشف التسلل (IDS) على الشبكة لكشف أي آليات هجوم غير اعتيادية وكشف أي انتهاكات أمنية لهذه الأنظمة عند كل حد من حدود شبكة <اسم الجهة>.
٣-٧	تثبيت أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (IDPS) على الشبكة لكشف أي حركة بيانات خبيثة على الشبكة عند كل حد من حدود شبكة <اسم الجهة>.
٣-٨	تثبيت تقنيات كشف/منع التهديدات المتقدمة المستمرة (APT) على الشبكة لكشف أو منع الهجمات على الشبكة والهجمات غير المعروفة مسبقًا عند كل حد من حدود شبكة <اسم الجهة>.
٣-٩	تثبيت جدار حماية التحقق من التطبيقات لحجب أي تطبيقات غير مدرجة في قائمة التطبيقات المسموحة أو غير معروفة أو لا تمتثل للضوابط الأمنية (مثل التطبيقات التي تتواصل عبر منفذ بروتوكول حزم بيانات المستخدم الخاص بنظام أسماء النطاقات "UDP/٥٣" وهي غير ممتثلة لبروتوكول نظام أسماء النطاقات (DNS)) عند كل حد من حدود شبكة <اسم الجهة>.
٣-١٠	تثبيت جدار الحماية لتطبيقات الويب (WAF) لتحليل وتصفية ومراقبة حركة البيانات، ومنع حركة بيانات من الإنترنت غير مصرح لها من وإلى تطبيقات الويب.
٣-١١	ضبط إعدادات بروتوكولات التشفير المقبولة والموافق عليها مثل بعض أنواع أمن طبقة النقل (TLS) للعمل على أي جهاز من أجهزة جدران الحماية لتطبيقات الويب (WAF) للتحقق من البيانات غير المشفرة. وفي حال عدم دعم الجهاز عملية تفريغ البيانات عبر أمن طبقة النقل، فلا بد من وضع جدار الحماية لتطبيقات الويب في جهاز فك تشفير للتحقق من البيانات غير المشفرة، أو تثبيت جدار الحماية لتطبيقات الويب على المستضيف.
٣-١٢	تفعيل خاصية جمع معلومات حركة البيانات عبر الشبكة (NetFlow) وتسجيل البيانات على كافة أجهزة حدود الشبكة.
٣-١٣	ضمان أن كافة أشكال حركة البيانات عبر الشبكة من أو إلى الإنترنت تمر عبر خادم وكيل طبقة التطبيقات المعتمدة والمجهز لتصفية الاتصالات غير المصرح بها.

٣-١٤	السماح للمستخدمين بالوصول إلى فئات عناوين (URL) محددة ومصرح بها، ومنع إمكانية الوصول إلى فئات العناوين (URL) الضارة أو المخصصة للاختراق، أو التي تعمل عبر خوادم مفوضة (Proxy) أو خوادم غير معروفة الهوية، أو المخصصة للتصيد أو المشبوهة أو غير المعروفة أو غير المصنفة.
٣-١٥	فك تشفير كافة حركة بيانات تصفح الإنترنت المشفرة عند الخادم المفوض (Proxy) على الحدود قبل تحليل المحتوى. يمكن لـ<اسم الجهة> استخدام قائمة محددة من التطبيقات لمواقع مسموحة يمكن الوصول إليها عبر خادم المفوض (Proxy) دون فك تشفير حركة البيانات.
٣-١٦	ضبط إعدادات الوصول وتسجيل الدخول عن بعد إلى شبكة <اسم الجهة> للقيام بتشفير البيانات قيد الاستخدام والنقل، واستخدام التحقّق من الهوية متعدّد العناصر.
٣-١٧	تثبيت جهاز وصول عن بعد يستخدم تقنيات مثل الشبكات الخاصة الافتراضية أو حلول طبقة المنافذ الآمنة-الشبكات الخاصة الافتراضية (SSL-VPN) لحجب وحماية كافة أشكال الوصول إلى شبكة <اسم الجهة>.
٣-١٨	مسح جميع الأجهزة التي تقوم بالدخول عن بعد إلى شبكة <اسم الجهة> قبل وصولها إلى الشبكة لضمان تطبيق جميع سياسات الأمن المعتمدة في <اسم الجهة> بنفس الطريقة التي تم تطبيقها على أجهزة الشبكة المحلية.
٣-١٩	تثبيت تقنيات كشف/منع هجمات حجب الخدمة (DoS) وهجمات تعطيل الخدمات الموزعة (DDoS) على أجهزة <اسم الجهة> أو من قبل أطراف خارجية لكشف وحجب هجمات حجب الخدمة (DoS) عند كل حد من حدود شبكة <اسم الجهة>.
٣-٢٠	تثبيت تقنيات أمن نظام أسماء النطاقات (DNS) لكشف ومنع الهجمات على نظام أسماء النطاقات عند كل حد من حدود شبكة <اسم الجهة>.
٣-٢١	تفعيل خاصية تسجيل الاستفسارات على نظام أسماء النطاقات (DNS) لكشف وتحديد اسم المستضيف للنطاقات الخبيثة المعروفة.
٣-٢٢	تثبيت بوابة أمن البريد الإلكتروني لكشف ومنع الهجمات عبر البريد الإلكتروني على حدود شبكة <اسم الجهة>.

٣-٢٣	ضمان التحديث المنتظم لكافة خدمات الاشتراك وفئات العناوين (URL) ومصادر المعلومات الاستباقية والقوائم المحددة من التطبيقات الممنوعة (Blacklists) والمؤشرات المعرفة المسبقة.
٤	القيود والضوابط
الهدف	الحد من مصادر الهجمات وحماية الشبكة الداخلية من التهديدات.
المخاطر المحتملة	يؤدي ضعف حماية الشبكة الداخلية والقيود والضوابط الخاصة بها إلى زيادة مخاطر التهديدات الداخلية والحركة الجانبية (Network Lateral Movement).
الإجراءات المطلوبة	
١-٤	ربط المنافذ والخدمات والأجهزة النشطة بأصول المعدات في قائمة جرد الأصول.
٢-٤	تقييد منافذ الشبكة وبروتوكولاتها والخدمات المتاحة على النظام وحصرها على متطلبات الأعمال لكل نظام.
٣-٤	القيام بعمليات مسح آلية للمنافذ بشكل منتظم على كافة الأنظمة، والتنبيه عند اكتشاف منافذ غير مصرح بها على النظام.
٤-٤	تفعيل جدار حماية المستضيف أو أدوات تصفية المنافذ لكل نظام مع تطبيق قاعدة المنع التلقائي التي تحجب جميع أشكال حركة البيانات باستثناء الخدمات والمنافذ المصرح لها فقط.
٥-٤	تثبيت جدار حماية لمركز البيانات لفحص ومراقبة الاتصالات عبر الشبكة المحلية الافتراضية (VLAN)، والمنافذ الموثوقة وغير الموثوقة، وما بين المناطق والأجزاء والخوادم لحماية الشبكات الداخلية وحجب الهجمات الداخلية.
٦-٤	إعداد سياسات جدار الحماية ونموذج القواعد لاتباع نموذج الأمن الإيجابي (نموذج السماح بقائمة محددة (whitelisting)) من خلال منع كافة أنواع حركة البيانات تلقائيًا والسماح فقط بحركة بيانات محددة إلى خدمات معينة. ويمكن تحقيق هذا الأمر من خلال ضبط إعدادات آخر قاعدة في قائمة التحكم بالوصول بحيث تحجب كافة أنواع حركة البيانات. ويمكن القيام بهذا الأمر بشكل صريح أو ضمني حسب المنصة.

٤-٧	إعداد جدار حماية لمركز البيانات مجهز بآلية التعرف على التطبيقات (المستوى ٤ - المستوى ٧) وآلية السماح بقائمة محددة (Whitelisting) ومنع قائمة محددة أخرى (Blacklisting).
٤-٨	ضبط إعدادات قوائم جدار الحماية بآلية التعرف على المستخدم لوضع السياسات بناءً على هوية المستخدم (UID).
٤-٩	في حال كانت شبكة <اسم الجهة> تعمل على الإصدار الرابع من بروتوكول الإنترنت (IPv٤)، يجب تطبيق ضوابط الأمن من المستوى ٢ لحماية الشبكة الداخلية.
٤-١٠	إعداد شبكات محلية افتراضية خاصة/معزولة لأجزاء الشبكة الحساسة أو الأجزاء المعزولة من الشبكة.
٤-١١	منع إمكانية وصول الشبكات أو أجزاء الأنظمة الحساسة إلى أي نظام في البيئة التقنية ما لم يتم مسحها مع تطبيق الضوابط الأمنية اللازمة والتحقق من الوضع الأمني للنظام.
٤-١٢	عزل شبكة الاتصالات من خلال وضعها في شبكات محلية افتراضية منفصلة وملائمة بناءً على وظيفتها مع استغلال الشبكات المحلية الافتراضية الخاصة أو التجزئة الدقيقة للشبكة.
٥	الوصول اللاسلكي
الهدف	تطبيق الضوابط الأمنية الملائمة لاستخدام الشبكات اللاسلكية وحمايتها.
المخاطر المحتملة	في حال تم ترك الشبكات اللاسلكية من دون حماية، ستتعرض <اسم الجهة> لمخاطر الاتصال غير المصرح به بالشبكة أو كشف البيانات.
الإجراءات المطلوبة	
٥-١	إجراء تقييم مخاطر شامل لتقييم مخاطر اتصال الشبكات اللاسلكية بالشبكة الداخلية.
٥-٢	الاحتفاظ بقائمة جرد بنقاط الوصول اللاسلكية المصرح بها والمتصلة بالشبكة السلكية.
٥-٣	إعداد أدوات مسح الثغرات الأمنية في الشبكة لكشف أو منع أي وصول لاسلكي غير مصرح به متصل بالشبكة السلكية والتنبيه بوجوده.
٥-٤	استخدام نظام كشف التسلل اللاسلكي (WIDS) لكشف أي وصول لاسلكي غير مصرح به متصل بالشبكة السلكية والتنبيه بوجوده.
٥-٥	إلغاء تفعيل الوصول اللاسلكي على الأجهزة التي لا تقتضي طبيعة عملها ذلك.

٥-٦	إعداد الوصول اللاسلكي على أجهزة المتصلين التي لا تحتاج لذلك لغايات العمل بحيث يتم السماح بالوصول إلى الشبكات اللاسلكية المصرح بها فقط وتقييد الوصول إلى الشبكات اللاسلكية الأخرى.
٥-٧	إلغاء تفعيل قدرات الشبكة اللاسلكية (المخصصة) لمشاركة الملفات بين الأجهزة مباشرة على الشبكات اللاسلكية لدى المتصلين.
٥-٨	إعداد نقاط الوصول اللاسلكية والأجهزة اللاسلكية للاتصال بالشبكة اللاسلكية باستخدام بروتوكولات آمنه مثل (WPA٣).
٥-٩	ضمان استخدام الشبكات اللاسلكية لبروتوكولات التحقق مثل بروتوكول المصادقة القابل للامتداد-أمن طبقة النقل (EAP/TLS) الذي يقتضي استخدام التحقّق من الهوية متعدّد العناصر بشكل متبادل.
٥-١٠	إلغاء تفعيل الوصول اللاسلكي للأجهزة الطرفية الموجودة على الأجهزة (مثل تقنية بلوتوث "Bluetooth" والاتصال قريب المدى "NFC") ما لم تقتضي طبيعة العمل ذلك.
٥-١١	إنشاء شبكات لاسلكية منفصلة للأجهزة الشخصية أو غير الموثوقة، والتعامل مع هذه الشبكات بحذر واعتبارها مصادرًا غير موثوقة مما يستدعي مراقبتها وتصفيتها بشكل مستمر.
٦	**التشفير**
الهدف	ضمان الحفاظ على سريّة حركة بيانات الشبكة والتأكّد من سريتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات المحمية.
المخاطر المحتملة	قد يؤدي عدم وجود التقنيات الأمنية المناسبة لضمان تشفير بيانات الشبكة إلى تعرض بيانات <اسم الجهة> لمخاطر سيبرانية نتيجة الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
٦-١	تطبيق أفضل معايير التشفير للشبكات وفقًا لمعيار التشفير المعتمد لدى <اسم الجهة>.
٦-٢	استخدام بروتوكولات الإدارة المشفرة الآمنة، مثل بروتوكول النقل الآمن (SSHv٢) وبروتوكول التحكم بسطح المكتب عن بعد (RDP) عبر أمن طبقة النقل (TLS).

٦-٣	تشفير حركة بيانات الشبكة الحساسة باستخدام الجيل التالي من خوارزميات التشفير المدعومة (مثل التشفير بمجموعة "Suite B") وفقًا لمعيار التشفير المعتمد في <اسم الجهة>.
٦-٤	تشفير حركة بيانات الوصول عن بعد عبر أمن بروتوكول الإنترنت (IPSec) أو أمن طبقة النقل (TLS) باستخدام الجيل التالي من خوارزميات التشفير المدعومة (مثل التشفير بمجموعة "Suite B") وفقًا لمعيار التشفير المعتمد لدى <اسم الجهة>.
٦-٥	إعداد بروتوكولات التطبيقات لتستخدم التشفير حيثما أمكن (مثل: بروتوكول نقل النص التشعبي الآمن "HTTPS" وبروتوكول النقل الآمن "FTPS" عبر طبقة المنافذ الآمنة "SSL"، وبروتوكول النفاذ إلى الدليل البسيط "LDAP" عبر طبقة المنافذ الآمنة "SSL").
٧	التحقق من سلامة البرمجيات والعتاد
الهدف	ضمان أن جميع برامج وعتاد الشبكة تأتي من مصادر شرعية وأنه لم يتم العبث بها والتحقق من ذلك.
المخاطر المحتملة	تعتبر الاختراقات في سلسلة الإمداد فرصة لتركيب وتثبيت البرامج والمعدات الخبيثة ضمن شبكة <اسم الجهة>، وقد تؤثر البرامج والعتاد الذي يتعرض لانتهاك أمني على أداء الشبكة ويهدد سرية وسلامة وتوافر المعلومات الخاصة ب<اسم الجهة>. ونتيجة لذلك، سيصبح من الممكن تحميل البرمجيات غير المصرح بها أو الخبيثة على الجهاز بعد تشغيلها.
الإجراءات المطلوبة	
٧-١	فحص كافة أجهزة الشبكة المادية للكشف عن أي علامات لوجود عبث عند التركيب.
٧-٢	الحصول على البرمجيات وتحديثات النظام وحزم التحديثات والإصلاحات والترقيات الخاصة بمكونات الشبكة من مصادر موثوقة.
٧-٣	أثناء تنزيل البرمجيات من الإنترنت، يجب التحقق من التجزئة مع قاعدة بيانات المورد لكشف أي تعديل غير مصرح به على البرامج الثابتة أو البرمجيات.
٧-٤	تطبيق واتباع عملية الرقابة على التغيير لأي تغييرات تنطوي على مخاطر كبيرة على شبكة <اسم الجهة>، بما في ذلك القواعد التي تسمح بتدفق حركة البيانات عبر أجهزة

	الشبكة وسياسات أمن جدران الحماية وترجمة عنوان الشبكة (NAT)، وغيرها. ويجب توثيق هذه العملية بما في ذلك العناصر التالية: • الغاية من القاعدة • الخدمات أو التطبيقات المتأثرة • المستخدمون والأجهزة المتأثرة • تاريخ إضافة القاعدة • تاريخ انتهاء صلاحية القاعدة، إذا كان ينطبق ذلك • اسم الشخص الذي أضاف القاعدة • بيان المشكلة • البيانات الداعمة • موافقة الإدارة على التغييرات
٨	معايير أخرى
الهدف	تطبيق جميع المعايير والمتطلبات الأمنية للشبكات لضمان أعلى مستويات الحماية.
المخاطر المحتملة	عدم تطبيق المعايير الأمنية المطلوبة لحماية الشبكة الخاصة بـ<اسم الجهة> يعرضها إلى تهديدات سيبرانية تهدف إلى تعطيل الأعمال والخدمات.
الإجراءات المطلوبة	
١-٨	تطبيق المعايير التالية: ١- معيار التعافي من الكوارث والنسخ الاحتياطية ٢- معيار تسجيل الأحداث وسجل التدقيق ٣- معيار الحماية المادية ٤- معيار الشبكات اللاسلكية ٥- معيار الإعدادات والتحصين ٦- المعايير الوطنية للتشفير

الأدوار والمسؤوليات

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

٢- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات>.

٤- **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

اختر التصنيف

الإصدار <١,٠>

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

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

٢- يجب على جميع العاملين في <اسم الجهة> الالتزام بهذا المعيار.

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