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 اللاسلكية

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

قائمة المحتويات

الغرض ٤
النطاق ٤
المعايير ٤
الأدوار والمسؤوليات ٨
التحديث والمراجعة ٨
الالتزام بالمعيار ٨

الغرض

يهدف هذا المعيار إلى تحديد متطلبات الأمن السيبراني التفصيلية لحماية أمن الشبكات اللاسلكية الخاصة بـ<اسم الجهة> وذلك لتحقيق الغرض الأساسي 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.

النطاق

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

المعايير

١	فصل الشبكة اللاسلكية
الهدف	ضمان حماية تصميم وبنية الشبكة اللاسلكية وحماية الأجزاء الشبكية وفقًا لمستوى الأمن الخاص بها.
المخاطر المحتملة	عدم فصل الشبكات اللاسلكية يعرض جميع الشبكات المتواجدة في نفس نطاق البث لنفس المخاطر 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	
١-١	تصميم وتطبيق شبكة لاسلكية معزولة منطقيًا و/أو ماديًا مع الأخذ بعين الاعتبار احتياجات الأعمال والمعمارية المؤسسية وذلك بالاستناد إلى مبدأ الدفاع الأمني متعدد المراحل ومبدأ المعمارية متعددة المستويات.
١-٢	تطبيق المستوى الملائم من ضوابط الأمن السيبراني على الأجزاء الشبكية المختلفة بناءً على قيمة وتصنيف المعلومات المعالجة في الشبكة اللاسلكية ومستويات الموثوقية والتأثير على الأعمال والمخاطر ذات العلاقة.
١-٣	تصميم وإعداد الشبكات اللاسلكية لتصفية مرور البيانات بين مختلف الأجزاء وحجب الوصول غير المصرح به.

١-٤	ضبط إعدادات جدار الحماية والموجّهات (Routers) لمنع أي اتصالات غير مصرح بها بين الشبكات اللاسلكية غير الموثوقة.
١-٥	مراجعة الإعدادات والقواعد والسياسات والملفات التعريفية الأمنية لجدران الحماية والموجهات (Routers) بشكل دوري بناءً على خطة معتمدة.
١-٦	منع الأنظمة الحساسة من الاتصال بالشبكة اللاسلكية.
٢	تأمين الحدود
الهدف	حماية حدود الشبكة اللاسلكية من التهديدات.
المخاطر المحتملة	ضعف تطبيق الضوابط الأمنية الملائمة لحماية حدود الشبكة اللاسلكية قد يجعلها عرضة للاختراق وفرض المزيد من التهديدات الخطيرة.
الإجراءات المطلوبة	
٢-١	الاحتفاظ بقائمة جرد محدثة لكافة حدود الشبكة اللاسلكية في <اسم الجهة>.
٢-٢	حظر الاتصالات مع عناوين بروتوكولات الإنترنت الضارة أو غير المستخدمة وحصر الوصول بمجالات عنوان بروتوكولات الإنترنت الموثوقة والضرورية عند كل حد من حدود الشبكة اللاسلكية ل<اسم الجهة>.
٢-٣	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 اللاسلكية عند كل حد من حدود الشبكة اللاسلكية <اسم الجهة>.
٢-٤	إعداد أنظمة المراقبة لتسجيل حزم بيانات الشبكة التي تمر عبر الحدود عند كل حد من حدود الشبكة اللاسلكية ل <اسم الجهة>.
٢-٥	تفعيل أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات على حدود الشبكة اللاسلكية للكشف عن أي حركة بيانات خبيثة على الشبكة عند كل حد من حدود شبكة <اسم الجهة>.
٢-٦	تثبيت تقنيات كشف/منع التهديدات المتقدمة المستمرة (APT) على الشبكة لكشف أو حجب الهجمات على الشبكة والهجمات غير المعروفة مسبقًا عند كل حد من حدود شبكة <اسم الجهة>.
٢-٧	تفعيل خاصية جمع معلومات حركة البيانات عبر الشبكة (NetFlow) وتفعيل سجلات الأحداث على كافة أجهزة حدود الشبكة اللاسلكية.

٢-٨	ضمان أن كافة أشكال حركة البيانات عبر الشبكة اللاسلكية من أو إلى الإنترنت تمر عبر خادم وكيل طبقة التطبيقات الموثقة والمجهز لتصفية الاتصالات غير المصرح بها.
٢-٩	تفعيل خاصية تسجيل الاستعلامات على نظام أسماء النطاقات (DNS) لكشف وتحديد اسم المستضيف للنطاقات الخبيثة المعروفة.
٢-١٠	ضمان التحديث المنتظم لكافة خدمات الاشتراك وفئات العناوين (URL) ومصادر المعلومات الاستباقية والقوائم المحددة من التطبيقات الممنوعة (Blacklists) والإشارات المعرفة المسبقة.
٣	**الارتباط اللاسلكي**
الهدف	ضبط استخدام الشبكات اللاسلكية وحمايتها.
المخاطر المحتملة	ضعف حماية الشبكات اللاسلكية قد يؤدي إلى تعرض <اسم الجهة> لمخاطر الاتصال غير المصرح به بالشبكة أو كشف البيانات.
الإجراءات المطلوبة	
٣-١	إجراء تقييم مخاطر شامل لتقييم مخاطر اتصال الشبكات اللاسلكية بالشبكة الداخلية.
٣-٢	الاحتفاظ بقائمة جرد بنقاط الوصول اللاسلكية المصرح بها والمتصلة بالشبكة السلكية.
٣-٣	إعداد أدوات مسح الثغرات الأمنية في الشبكة لكشف أي محاولة اتصال نقاط وصول لاسلكية غير مصرح به بالشبكة السلكية والتنبيه بوجودها.
٣-٤	استخدام نظام كشف التسلل اللاسلكي (WIDS) لكشف أي محاولة اتصال نقاط وصول لاسلكية غير مصرح به بالشبكة السلكية والتنبيه بوجودها.
٣-٥	إلغاء تفعيل الوصول اللاسلكي على الأجهزة التي لا تقتضي طبيعة عملها ذلك.
٣-٦	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.
٣-٧	إلغاء تفعيل قدرات الشبكة اللاسلكية (المخصصة) لمشاركة الملفات بين الأجهزة مباشرة على الشبكات اللاسلكية لدى المتصلين.

٣-٨	إعداد نقاط الوصول اللاسلكية والأجهزة اللاسلكية للاتصال بالشبكة اللاسلكية باستخدام بروتوكولات آمنه مثل (WPA٣).
٣-٩	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.
٣-١٠	إلغاء تفعيل الوصول اللاسلكي للأجهزة الطرفية الموجودة على الأجهزة (مثل تقنية بلوتوث "Bluetooth" والاتصال قريب المدى "NFC") ما لم تقتضي طبيعة العمل ذلك.
٣-١١	إنشاء شبكات لاسلكية منفصلة للأجهزة الشخصية أو غير الموثوقة، والتعامل مع هذه الشبكات بحذر واعتبارها مصادرًا غير موثوقة مما يستدعي مراقبتها وتصفيتها بشكل مستمر.
٣-١٢	تقييد نقل البيانات المصنفة سري وسري للغاية عبر الشبكات اللاسلكية.
٤	التحقق من سلامة البرمجيات والعتاد
الهدف	ضمان أن جميع برامج وعتاد الشبكة تأتي من مصادر أصلية 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	
٤-١	قبل التركيب يجب فحص كافة أجهزة الشبكة اللاسلكية المادية بحثًا عن أي علامات عبث.
٤-٢	الحصول على البرمجيات وتحديثات النظام وحزم التحديثات والإصلاحات والترقيات الخاصة بمكونات الشبكة اللاسلكية من مصادر الشركة المصنعة.
٥	معايير أخرى

الهدف	تطبيق جميع المعايير والمتطلبات الأمنية للشبكات اللاسلكية لضمان أعلى مستويات الحماية.
المخاطر المحتملة	عدم تطبيق جميع المعايير والمتطلبات الأمنية يعرض <اسم الجهة> إلى زيادة في المخاطر الأمنية للشبكات اللاسلكية.
الإجراءات المطلوبة	
١-٥	تطبيق المعايير التالية: ١- معيار النسخ الاحتياطي والتعافي ٢- معيار تسجيل الأحداث وسجل التدقيق ٣- معيار الحماية المادية ٤- معيار أمن الشبكات ٥- معيار إدارة هويات الدخول والصلاحيات ٦- معيار الإعدادات والتحصين ٧- معيار التشفير ٨- معيار إدارة حوادث وتهديدات الأمن السيبراني

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>.

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>.