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:

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

يهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو 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

يغطي هذا المعيار جميع أنظمة الشبكات التقنية اللاسلكية الخاصة بـ<اسم الجهة>، وينطبق على جميع العاملين في <اسم الجهة>.

المعايير

1	الوصول الآمن (Secure Access)
الهدف	ضمان تطبيق الإعدادات الصحيحة للوصول إلى واجهات إدارة أمن الشبكات اللاسلكية من أجل حمايتها بشكل فعال من الهجمات السيبرانية.
المخاطر المحتملة	تؤدي الإعدادات غير الكافية لحلول واجهات إدارة أمن الشبكات اللاسلكية إلى تعرضها داخل بيئة <اسم الجهة> إلى هجمات أو انتهاكات أمنية.
الإجراءات المطلوبة	
1-1	إعداد قوائم الوصول بصورة تسمح بالتحكم بالوصول إلى أجهزة اتصالات الشبكة اللاسلكية بحيث يمكن للأشخاص المصرح لهم فقط الوصول إلى هذه الأجهزة. Access lists shall be configured to control access to wireless network communication devices and ensure that these devices are accessible to authorized users only.
2-1	استخدام آلية تحقق مركزية للتحقق من جميع المستخدمين التفاعليين الذين يقومون بعمل تغييرات على كافة أجهزة الشبكة اللاسلكية. كما يجب أن تكون أنظمة التحقق بأقل عدد ممكن. Centralized user-level authentication shall be deployed to authenticate all interactive users making changes to all

wireless network devices. Additionally, authentication systems shall be as few as possible.	
أن يقتصر 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 لاسلكياً. Restrict wireless network administrators' access to use dedicated Privileged Access Workstations (PAWs) or jump servers placed in an out-of-band management network, segmented from <entity name>'s network and isolated from the internet, and not wirelessly.	3-1
تطبيق التحقّق من هوية الوصول متعدّد العناصر لمشرفي الأنظمة اللاسلكية، واستخدام الجلسات المشفرة لإدارة وإعداد مكونات أجهزة الشبكات اللاسلكية. Multi-Factor Authentication shall be implemented and encrypted sessions shall be used to manage (or administrate) all wireless network devices by administrators.	4-1
تقييد استخدام كلمة المرور الاساسية بتعليمات وإجراءات معتمدة، وحصره على مشرفين محددين فقط بحسب ما هو ضروري لغايات غير تشغيلية، أو لغرض استعادة أجهزة الشبكة اللاسلكية التي تم فصلها عن الشبكة. The use of hard-coded passwords shall be limited to relevant administrators only as necessary for non-interactive purposes, as well as to recover wireless network devices that have become disconnected from the network.	5-1
إعداد أجهزة الشبكة اللاسلكية لعرض رسالة نصية تنبيهية عند تسجيل الدخول. ويجب ألا تُظهر هذه الرسالة النصية الخصائص الأساسية للشبكة. Wireless network devices shall be configured to display an alert banner at login. This banner text shall not provide the underlying characteristics of the network.	6-1
فصل الشبكة اللاسلكية (Wireless Network Segregation)	2
ضمان حماية تصميم وبنية الشبكة اللاسلكية وحماية الأجزاء الشبكية وفقاً لمستوى الأمن الخاص بها.	الهدف

المخاطر المحتملة	تتشارك الشبكات اللاسلكية 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	
1-2	تصميم وتطبيق شبكة لاسلكية معزولة منطقياً و/أو مادياً مع الأخذ بعين الاعتبار احتياجات الأعمال والمعمارية المؤسسية وذلك بالاستناد إلى الدفاع الأمني متعدد المراحل والمعمارية متعددة المستويات. A logically and/or physically segmented wireless network shall be designed and implemented, taking into consideration business needs and enterprise architecture, and based on the principles of defense-in-depth and multi-tier architecture.
2-2	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 المرافقة. Appropriate level of security controls shall be applied to different network segments based on the value and classification of information processed in the wireless network, levels of trust, business impact and associated risks.
3-2	تصميم وإعداد الشبكات اللاسلكية لتصفية مرور البيانات بين مختلف الأجزاء وحجب الوصول غير المصرح به. Wireless networks shall be designed and configured to filter traffic between different segments and block any unauthorized access.
4-2	إعداد جدران الحماية والموجّهات (Routers) لمنع أي اتصالات غير مصرح بها بين الشبكات اللاسلكية غير الموثوقة Firewalls and routers shall be configured to prevent any unauthorized connections between untrusted wireless networks
5-2	منع الأنظمة الحساسة من الاتصال بالشبكة اللاسلكية.

	Critical systems shall be prevented from connecting to the wireless network.
6-2	مراجعة الإعدادات والقواعد والسياسات والملفات التعريفية الأمنية لجدران الحماية والموجهات (Routers) بشكل دوري. Security configurations, rules, policies and profiles for firewalls and routers shall be reviewed in regular bases.
3	تأمين الحدود (Boundary Defense)
الهدف	حماية حدود الشبكة اللاسلكية من التهديدات.
المخاطر المحتملة	في حال تم ترك حدود الشبكة اللاسلكية من دون الحماية التي توفرها الضوابط الأمنية المناسبة، سيتمكن المهاجمون من اختراق الشبكة اللاسلكية بسهولة وفرض المزيد من التهديدات الخطيرة.
الإجراءات المطلوبة	
1-3	الاحتفاظ بقائمة جرد محدثة لكافة حدود الشبكة اللاسلكية في <اسم الجهة>. An up-to-date inventory of all of <entity name>'s wireless network boundaries shall be maintained.
2-3	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 لـ<اسم الجهة>. Communications with known malicious or unused Internet IP addresses shall be denied, and access shall be limited to trusted and necessary IP address ranges at each of <entity name>'s wireless network boundaries.
3-3	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>. Communication over unauthorized TCP or UDP ports or application traffic shall be denied to ensure that only authorized protocols are allowed to cross the network boundary in or out of the wireless network at each of <entity name>'s network boundaries.

4-3	إعداد أنظمة المراقبة لتسجيل حزم بيانات الشبكة التي تمر عبر الحدود عند كل حد من حدود الشبكة اللاسلكية لـ <اسم الجهة>. Monitoring systems shall be configured to record network packets passing through the boundary at each of <entity name>'s wireless network boundaries.
5-3	تفعيل أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات على حدود الشبكة اللاسلكية لكشف أي حركة بيانات خبيثة على الشبكة عند كل حد من حدود شبكة <اسم الجهة>. Network-based Intrusion Prevention Systems (IPS) shall be deployed to block malicious network traffic at each of <entity name>'s wireless network boundaries.
6-3	تثبيت تقنيات كشف/منع التهديدات المتقدمة المستمرة (APT) على الشبكة لكشف أو حجب الهجمات على الشبكة والهجمات غير المعروفة مسبقاً عند كل حد من حدود شبكة <اسم الجهة>. Network-based Advanced Persistent Threat (APT) detection/prevention systems shall be deployed to detect or block malicious network attacks and zero-day attacks at each of <entity name>'s network boundaries.
7-3	تمكين جمع معلومات حركة البيانات عبر الشبكة (NetFlow) وتسجيل البيانات على كافة أجهزة حدود الشبكة اللاسلكية. The collection of NetFlow and logging data shall be enabled on all wireless network boundary devices.
8-3	ضمان أن كافة أشكال حركة البيانات عبر الشبكة اللاسلكية من أو إلى الإنترنت تمر عبر خادم وكيل طبقة التطبيقات المعتمدة والمجهز لتصفية الاتصالات غير المصرح بها. All wireless network traffic to/from the Internet shall pass through an authenticated application layer proxy that is configured to filter unauthorized connections.
9-3	تمكين تسجيل الاستفسارات على نظام أسماء النطاقات لكشف وتحديد اسم المستضيف للنطاقات الخبيثة المعروفة. Domain Name System (DNS) query logging shall be enabled to detect hostname lookups for known malicious domains.

10-3	ضمان التحديث المنتظم لكافة خدمات الاشتراك وفئات العناوين (URL) ومصادر المعلومات الاستباقية والقوائم المحددة من التطبيقات الممنوعة (Blacklists) والإشارات المعرفة المسبقة. All subscription services, URL categories, threat feeds, blacklists, and signatures shall be up-to-date and updated regularly.
5	الارتباط اللاسلكي (Wireless Access)
الهدف	ضبط استخدام 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	
1-5	إجراء تقييم مخاطر شامل لتقييم مخاطر اتصال الشبكات اللاسلكية بالشبكة الداخلية. A comprehensive risk assessment exercise shall be conducted to evaluate the risks of connecting wireless networks to the internal network.
2-5	الاحتفاظ بقائمة جرد بنقاط الوصول اللاسلكية المصرح بها والمتصلة بالشبكة السلكية. An inventory of authorized wireless access points connected to the wired network shall be maintained.
3-5	إعداد أدوات مسح الثغرات الأمنية في الشبكة لكشف أو منع أي وصول لاسلكي غير مصرح به متصل بالشبكة السلكية والتنبيه بوجوده. Network vulnerability scanning tools shall be configured to detect and alert on unauthorized wireless access points connected to the wired network.
4-5	استخدام نظام كشف التسلل اللاسلكي (WIDS) لكشف أي وصول لاسلكي غير مصرح به متصل بالشبكة السلكية والتنبيه بوجوده. Wireless Intrusion Detection System (WIDS) shall be used to detect/prevent and alert on unauthorized wireless access points connected to the wired network.
5-5	إلغاء تفعيل الوصول اللاسلكي على الأجهزة التي لا تقتضي طبيعة عملها ذلك.

Wireless access on devices that do not have a business purpose for wireless access shall be disabled.	
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. Wireless access on client machines that do not have a business need for wireless access shall be configured to allow access to authorized wireless networks only, and to restrict access to other wireless networks.	6-5
إلغاء تفعيل قدرات الشبكة اللاسلكية (المخصصة) لمشاركة الملفات بين الأجهزة مباشرة على الشبكات اللاسلكية لدى المتصلين. Peer-to-peer (ad hoc) wireless network capabilities shall be disabled on wireless clients.	7-5
إعداد نقاط الوصول اللاسلكية والأجهزة اللاسلكية للاتصال بالشبكة اللاسلكية باستخدام بروتوكولات آمنه مثل (WPA2) أو (WPA3). Wireless access points and wireless devices shall be configured to connect to the wireless network using secure protocol such as WPA2 or WPA3.	8-5
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. Wireless networks shall use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) that requires mutual Multi-Factor Authentication.	9-5
إلغاء تفعيل الوصول اللاسلكي للأجهزة الطرفية الموجودة على الأجهزة (مثل تقنية بلوتوث "Bluetooth" والاتصال قريب المدى "NFC") ما لم تقتضي طبيعة العمل ذلك. Wireless access of peripheral devices (such as Bluetooth and NFC) shall be disabled unless such access is required for a business purpose.	10-5

11-5	إيجاد شبكات لاسلكية منفصلة للأجهزة الشخصية أو غير الموثوقة، والتعامل مع هذه الشبكات بحذر واعتبارها مصادراً غير موثوقة مما يستدعي مراقبتها وتصفيتها بشكل مستمر. A separate wireless network shall be created for personal or untrusted devices. Enterprise access from this network shall be treated as untrusted and shall be filtered and audited accordingly.
7	الأمن المادي (Physical Security)
الهدف	ضمان حماية جميع أجهزة الشبكة اللاسلكية المطلوبة لاتصالات الشبكة من العبث أو التعديل أو أي هجمات مادية أخرى.
المخاطر المحتملة	يمكن أن يؤدي الهجوم المادي على أجهزة الشبكة اللاسلكية التي تحفظ عمليات الاتصالات إلى الإضرار بالأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة>، وبالتالي التأثير على سير أعمالها المعتاد. في حال تلف الجهاز أو العبث به أو تعديله مادياً، لا يمكن لـ<اسم الجهة> الوثوق بالمعلومات المرسلة عبره وسيرتفع مستوى المخاطر التي قد تهدد أمن الشبكة.
الإجراءات المطلوبة	
1-7	تطبيق ضوابط الوصول المادي على كافة أجهزة الشبكة اللاسلكية All network devices that are required for network communications shall be placed in a secured area with physical access controls implemented.
8	التسجيل والمراقبة (Logging and Monitoring)
الهدف	ضمان مراقبة وتخزين كافة الأحداث الحساسة المتعلقة بأمن الشبكة اللاسلكية من أجل الاكتشاف الاستباقية للهجمات السيبرانية وإدارة المخاطر بفعالية لمنع أو تقليل الآثار المترتبة على أعمال <اسم الجهة>.
المخاطر المحتملة	لضمان سلامة الشبكة اللاسلكية، يجب مراقبة كافة أجهزة الشبكة بشكل منتظم وضمان إمكانية الوصول إليها من قبل فرق الأمن السيبراني في <اسم الجهة>. دون القدرة على مراقبة وتسجيل الأحداث في الشبكة، لن تتمكن <اسم الجهة> من التحقيق في الهجمات التي يتعرض لها أمن الشبكة اللاسلكية مما يؤدي إلى زيادة تكرار تلك الهجمات.
الإجراءات المطلوبة	

1-8	إعداد كافة أجهزة الأمن والشبكة اللاسلكية لتسجيل سجلات الأحداث والتدقيق في نظام إدارة الأحداث والسجلات المركزي لأغراض التحليل والربط والتنبيه وفقاً لمعيار إدارة ومراقبة سجل الأحداث المعتمد في <اسم الجهة>. All wireless network and security devices shall be configured to log events and audit logs to the central event and log management system for analysis, correlation and alerting as per <entity name>'s Event Log Management and Monitoring Standard.
2-8	ضمان اتساق كافة سجلات الأجهزة مع متطلبات معيار إدارة ومراقبة سجل الأحداث المعتمد في <اسم الجهة>. All device logs shall be consistent with the requirements of <entity name>'s Event Log Management and Monitoring Standard.
3-8	إعداد أجهزة الشبكة اللاسلكية لإرسال الأحداث المتعلقة بمحاولات الدخول الناجحة وغير الناجحة إلى واجهات الإدارة إلى نظام إدارة الأحداث والسجلات المركزي لأغراض التحليل والربط والتنبيه. Wireless network devices shall be configured to send events related to failed and successful login to administration interfaces to the central event and log management system for analysis, correlation and alerting.
9	الإعدادات والتحصين (Secure Configuration)
الهدف	لضمان إيجاد ومعالجة الثغرات في أجهزة الشبكة والتحصين الامن لها.
المخاطر المحتملة	لضمان سلامة الشبكة اللاسلكية <اسم الجهة>، يجب عمل اختبارات أمنية، وتطبيق التحديثات وتحصين الاعدادات والتحديث المستمر لمعالجة المخاطر والتهديدات.
الإجراءات المطلوبة	
1-9	إجراء اختبارات أمنية دورية (مثل تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسة إدارة الثغرات الأمنية المتّبعة في <اسم الجهة>. Regular security testing, such as vulnerability assessments and penetration testing, shall be performed as per <entity name>'s Vulnerability Management Policy.

2-9	إجراء التحديثات والإصلاحات على أجهزة الشبكات اللاسلكية بشكل منتظم وفقاً لسياسة إدارة التحديثات والإصلاحات في <اسم الجهة> لضمان تحديث جميع البرامج الثابتة على الأجهزة وتطبيق التحديثات والإصلاحات. Network devices shall be regularly patched and updated as per <entity name>'s Patch Management Policy to ensure all devices firmware is up-to-date and all patches are applied.
3-9	إزالة/إلغاء تفعيل الخدمات غير الضرورية أو غير اللازمة على أجهزة الشبكة مثل: بروتوكول النقل الآمن (FTP) أو بروتوكول تل نت (Telnet) أو غيرها. Unnecessary/unrequired services on network devices, such as FTP, Telnet, etc., shall be removed/disabled.
4-9	إعداد وضبط كافة أجهزة الشبكة ليتزامن وقتها مع ثلاث خوادم زمنية إضافية على الأقل. All network devices shall be configured to synchronize clock with at least three centralized time sources.
5-9	التحديث المستمر لبرامج تشغيل الموجهات Keep the router's Firmware Up to Date
10	التحقق من سلامة البرمجيات والمعدات (Hardware and Software Integrity Validation)
الهدف	ضمان أن جميع برامج ومعدات الشبكة اللاسلكية 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> اللاسلكية، وقد تؤثر البرامج والمعدات التي تتعرض لانتهاك أمني على أداء الشبكة وتهدد سرية وسلامة وتوافر المعلومات الخاصة بـ<اسم الجهة>. ونتيجة لذلك، سيصبح من الممكن تحميل البرمجيات غير المصرح بها أو الخبيثة على الجهاز بعد تشغيلها.
الإجراءات المطلوبة	
1-10	فحص كافة أجهزة الشبكة اللاسلكية المادية بحثاً عن أي علامات لوجود عبث عند التركيب. All physical wireless network devices shall be scanned for signs of tampering upon installation.

2-10	الحصول على البرمجيات وتحديثات النظام وحزم التحديثات والإصلاحات والترقيات الخاصة بمكونات الشبكة اللاسلكية من مصادر الشركة المصنعة. Software, updates, patches, and upgrades to wireless network components shall be obtained from validated sources.

الأدوار والمسؤوليات

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

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

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

الالتزام بالمعيار

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

2- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا المعيار.

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