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

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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.

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 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 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 من أجل حمايتها بشكل فعال من الهجمات السيبرانية.
المخاطر المحتملة	تؤدي الإعدادات غير الكافية لحلول واجهات إدارة أمن الشبكات إلى تعرض أجهزة الشبكات داخل بيئة <اسم الجهة> إلى هجمات أو انتهاكات أمنية.
الإجراءات المطلوبة	
1-1	إعداد قوائم الوصول بصورة تسمح بالتحكم بالوصول إلى أجهزة اتصالات الشبكة بحيث يمكن للأشخاص المصرح لهم فقط الوصول إلى هذه الأجهزة. Access lists shall be configured to control access to network communication devices and ensure that these devices are accessible to authorized users only.
2-1	إعداد قائمة وصول لحماية جميع أجزاء الشبكة من انتحال عنوان بروتوكول الإنترنت (IP Address Spoofing). An access list shall be configured to protect all network segments from Layer-3 IP address spoofing.

3-1	استخدام آلية تحقق مركزية للتحقق من جميع المستخدمين التفاعليين الذين يقومون بعمل تغييرات على كافة أجهزة الشبكة. 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 network devices. Additionally, authentication systems shall be as few as possible.
4-1	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.
5-1	تطبيق التحقّق من الهوية متعدّد العناصر واستخدام الجلسات المشفرة لإدارة كافة أجهزة الشبكات. Multi-Factor Authentication shall be implemented and encrypted sessions shall be used to manage all network devices.
6-1	تقييد استخدام كلمة المرور المحددة بتعليمات ثابتة وحصره على مشرفين محددين فقط بحسب ما هو ضروري لغايات غير تفاعلية ولاستعادة أجهزة الشبكة 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 network devices that have become disconnected from the network.
7-1	إعداد أجهزة الشبكة لعرض رسالة نصية تنبيهية عند تسجيل الدخول. ويجب ألا تُظهر هذه الرسالة النصية الخصائص الأساسية للشبكة. Network devices shall be configured to display an awareness banner at login. This banner text shall not provide the underlying characteristics of the network.

2	فصل الشبكة (Network Segregation)
الهدف	ضمان حماية تصميم وبنية الشبكة وحماية الأجزاء الشبكية وفقاً لمستوى الأمن الخاص بها.
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	
1-2	تصميم وتطبيق شبكة 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 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 المخزنة أو المعالجة في الشبكة 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 stored or processed in the network, levels of trust, business impact and associated risks.
3-2	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) وفقاً للبنية المؤسسية والبنية الأمنية في <اسم الجهة>.

اختر التصنيف

Multi-tier architecture protected by dual layer of firewalls shall be implemented. Specifically, the network shall be segmented into three or more layers (boundary/perimeter, core and trusted) and the network segments shall be divided into zones (demilitarized zone “DMZ”, management zone, production zone, database zone, development/testing zone, etc.) as per <entity name>’s enterprise architecture and security architecture.	
تصميم وإعداد الشبكات لتصفية مرور البيانات بين مختلف الأجزاء وحجب الوصول غير المصرح به. Networks shall be designed and configured to filter traffic between different segments and block any unauthorized access.	4-2
وضع الخوادم أو مخازن البيانات التي تتضمن معلومات محمية في أجزاء شبكية منفصلة ومخصصة. Servers or data stores with sensitive information shall be placed in dedicated separate network segments.	5-2
إعداد جدران الحماية والموجّهات (Routers) لمنع أي اتصالات غير مصرح بها بين الشبكات غير الموثوقة وأي مكونات نظام تقوم بتخزين معلومات حساسة أو حساسة جداً. Firewalls and routers shall be configured to prevent any unauthorized connections between untrusted networks and any system components storing highly confidential or confidential information.	6-2
تحديد وتطبيق المستويات والحدود لكل منطقة أمنية. Levels and boundaries shall be defined and implemented for each security zone.	7-2
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). An out-of-band management network zone or segment, including all administration servers, machines with administrative access, Secure Shell (SSH) servers, jump	8-2

servers and Privileged Access Workstations (PAWs), shall be defined and implemented.	
فصل الشبكات اللاسلكية عن الشبكة الداخلية والشبكات المعزولة والشبكات الخاصة. Wireless networks shall be segregated from the internal network, isolated networks and private networks.	9-2
تحديد الخوادم والشبكات وبيئات الإنتاج والاختبار والبيئات الموثوقة المستخدمة في تطوير واختبار وفحص وتخزين البيانات والنشاطات ذات الصلة بوضوح وفصلها عن الشبكات الأخرى. Servers, networks and production, test, and trusted environments used for developing, testing, scanning and storing data and any other related activities, shall be clearly identified and segregated from other networks.	10-2
فصل أجزاء الأنظمة الحساسة منطقياً عن البيئات الأخرى. Segments of critical systems shall be logically isolated from other environments.	11-2
منع الأنظمة الحساسة من الاتصال بالشبكة اللاسلكية. Critical systems shall be prevented from connecting to the wireless network.	12-2
منع الأنظمة الحساسة من الاتصال بالإنترنت في حال كانت هذه الأنظمة تقدم خدمات داخلية لا تحتاج إلى صلاحية الوصول عن بعد أو الوصول عبر الإنترنت. Critical systems that offer internal services which do not require remote or Internet access shall be prevented from connecting to the Internet	13-2
مراجعة الإعدادات والقواعد والسياسات والملفات التعريفية الأمنية لجدران الحماية والموجهات (Routers) التي تدعم الشبكات الحساسة مرة كل ستة أشهر على الأقل. Security configurations, rules, policies and profiles for firewalls and routers that support critical networks shall be reviewed at least every six months.	14-2
تأمين الحدود (Boundary Defense)	3
حماية حدود الشبكة من التهديدات.	الهدف

اختر التصنيف

المخاطر المحتملة	في حال تم ترك حدود الشبكة من دون الحماية التي توفرها الضوابط الأمنية المناسبة، سيتمكن المهاجمون من اختراق الشبكة بسهولة وفرض المزيد من التهديدات الخطيرة.
الإجراءات المطلوبة	
1-3	الاحتفاظ بقائمة جرد محدثة لكافة حدود الشبكة في <اسم الجهة>. An up-to-date inventory of all of <entity name>'s network boundaries shall be maintained.
2-3	القيام بعمليات مسح وفحص منتظمة من الخارج لكل حد شبكة موثوق لاكتشاف أي اتصالات غير مصرح بها يمكن الوصول إليها عبر الحدود. Regular scans from outside each trusted network boundary shall be performed to detect any unauthorized connections that can be accessed across the boundary.
3-3	حظر الاتصالات مع عناوين بروتوكولات الإنترنت الخبيثة أو غير المستخدمة وحصر الوصول بمجالات عنوان بروتوكولات الإنترنت الموثوقة والضرورية عند كل حد من حدود شبكة <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 network boundaries.
4-3	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 عبر حدود الشبكة عند كل حد من حدود شبكة <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 network at each of <entity name>'s network boundaries.
5-3	إعداد أنظمة المراقبة لتسجيل حزم بيانات الشبكة التي تمر عبر الحدود عند كل حد من حدود شبكة <اسم الجهة>.

Monitoring systems shall be configured to record network packets passing through the boundary at each of <entity name>'s network boundaries.	
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>. Network-based Intrusion Detection Systems (IDS) sensors shall be deployed to detect any unusual attack mechanisms and detect any compromise of these systems at each of <entity name>'s network boundaries.	6-3
تثبيت أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات على الشبكة 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 network boundaries.	7-3
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.	8-3
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/53" وهي غير ممتثلة لبروتوكول نظام أسماء النطاقات) عند كل حد من حدود شبكة <اسم الجهة>. Application inspection firewall shall be deployed to block applications that are not whitelisted, unknown or non-compliant with security controls (for example, applications communicating over UDP/53 while not being compliant with DNS protocol) at each of <entity name>'s network boundaries.	9-3

10-3	تثبيت جدار الحماية لتطبيقات الويب (WAF) لتحليل وتصفية ومراقبة حركة البيانات، ومنع حركة بيانات غير المصرح لها من وإلى تطبيقات الويب. Web Application Firewall (WAF) shall be placed to analyzes, filters, monitors, and blocks Internet traffic to and from a web application.
11-3	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. Acceptable and approved encryption protocols such as some types of Transport Layer Security (TLS) shall be configured to terminate on any WAF device to inspect decrypted traffic. If the device does not support TLS offloading, WAF shall sit behind a decryption device to inspect decrypted traffic. Otherwise, a host-based web application firewall shall be deployed.
12-3	تمكين جمع معلومات حركة البيانات عبر الشبكة (NetFlow) وتسجيل البيانات على كافة أجهزة حدود الشبكة. The collection of NetFlow and logging data shall be enabled on all network boundary devices.
13-3	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. All network traffic to/from the Internet shall pass through an authenticated application layer proxy that is configured to filter unauthorized connections.
14-3	السماح للمستخدمين بالوصول إلى فئات عناوين (URL) محددة ومصرح بها، وحجب إمكانية الوصول إلى فئات العناوين (URL) الضارة أو المخصصة للاختراق، أو التي تعمل عبر خوادم مفوضة أو خوادم غير معروفة الهوية، أو المخصصة للتصيد أو المشبوهة أو غير المعروفة أو غير المصنفة. Only specific and whitelisted URL categories shall be allowed to users. Access to hacking, malware, proxy, anonymizers,

phishing, suspicious, unknown and uncategorized URLs shall be disabled.	
فك تشفير كافة حركة بيانات تصفح الإنترنت المشفرة عند الخادم المفوض على الحدود قبل تحليل المحتوى. يمكن لـ<اسم الجهة> استخدام قائمة محددة من التطبيقات لمواقع مسموحة يمكن الوصول إليها عبر خادم وكيل دون فك تشفير حركة البيانات. All encrypted Internet browsing traffic at the boundary proxy shall be decrypted prior to analyzing the content. However, <entity name> may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	15-3
ضبط إعدادات الوصول وتسجيل الدخول عن بعد إلى شبكة <اسم الجهة> للقيام بتشفير البيانات قيد الاستخدام والنقل، واستخدام التحقّق من الهوية متعدّد العناصر. All remote login access to <entity name>'s network shall be configured to encrypt data in transit. Additionally, Multi-Factor Authentication shall be used.	16-3
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>. A remote access device that uses technologies such as Virtual Private Network (VPN), or SSL-VPN solutions shall be deployed to terminate and protect all remote access to <entity name>'s network.	17-3
مسح جميع أجهزة المشاريع 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. All enterprise devices remotely logging into <entity name>'s network shall be scanned prior to accessing the network to ensure that all of <entity name>'s security policies have been enforced in the same manner used on local network devices.	18-3
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>. Denial of Service (DoS) and Distributed DoS (DDoS) detection/prevention technologies shall be deployed (on prim	19-3

اختر التصنيف

	or by a third party) to detect or block DoS attacks at each of <entity name>'s network boundaries.
20-3	تثبيت تقنيات أمن نظام أسماء النطاقات لكشف أو حجب الهجمات على نظام أسماء النطاقات عند كل حد من حدود شبكة <اسم الجهة>. Domain Name System (DNS) security technologies shall be deployed to detect or block DNS attacks at each of <entity name>'s network boundaries.
21-3	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.
22-3	تثبيت بوابة أمن البريد الإلكتروني لكشف أو حجب الهجمات عبر البريد الإلكتروني على حدود شبكة <اسم الجهة>. Email security gateway shall be deployed to detect or block email-based attacks at each of <entity name>'s network boundaries.
23-3	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.
4	القيود والضوابط (Limitations and Controls)
الهدف	الحد من مصادر الهجمات وحماية الشبكة الداخلية من التهديدات.
المخاطر المحتملة	تؤدي حماية الشبكة الداخلية إلى تقليل مخاطر التهديدات الداخلية والحركة الجانبية (Network Lateral Movement).
الإجراءات المطلوبة	
1-4	ربط المنافذ والخدمات والأجهزة النشطة بأصول المعدات في قائمة جرد الأصول. Active ports, services and protocols shall be associated with the hardware assets in the asset inventory.

2-4	تقييد منافذ الشبكة وبروتوكولاتها والخدمات المتاحة على النظام وحصرها على متطلبات الأعمال لكل نظام. Only network ports, protocols, and services listening on a system with validated business needs shall be running on each system.
3-4	القيام بعمليات مسح آلية للمنافذ بشكل منتظم على كافة الأنظمة، والتنبيه عند اكتشاف منافذ غير مصرح بها على النظام. Automated port scans shall be performed on a regular basis against all systems, and alerts shall be raised upon the detection of unauthorized ports on a system.
4-4	تطبيق 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. Host-based firewalls or port filtering tools shall be applied on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
5-4	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. A datacenter firewall shall be deployed to inspect and monitor inter-VLAN, trust-to-untrust, zone-to-zone, segment-to-segment, and east-west communications to protect the internal network and block internal attacks.
6-4	إعداد سياسات جدار الحماية ونموذج القواعد لاتباع نموذج الأمن الإيجابي (نموذج السماح بقائمة محددة من التطبيقات) من خلال حجب كافة أنواع حركة البيانات تلقائياً 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. Firewall policies and rules model shall be configured to follow positive security model (whitelisting model) by blocking all traffic by default and only allowing specific traffic to identified services. This can be achieved by configuring the last rule in

an access control list to deny all traffic. In addition, this can be performed explicitly or implicitly, depending on the platform.	
إعداد جدار حماية لمركز البيانات مجهز بآلية التعرف على التطبيقات (المستوى 4-المستوى 7) وآلية السماح بقائمة محددة من التطبيقات (Whitelisting) ومنع قائمة محددة أخرى من التطبيقات (Blacklisting). Datacenter firewall shall be configured with application identification (Layer4-Layer7), and application whitelisting and blacklisting.	7-4
ضبط إعدادات قوائم جدار الحماية بآلية التعرف على المستخدم لوضع السياسات بناءً على هوية المستخدم (UID). Firewall rules shall be configured with user identification to build policies based on User Identity (UID).	8-4
تطبيق الضوابط 3-6 إلى 3-10 المذكورة أعلاه في هذا المعيار على الشبكة الداخلية. Controls 3-6 to 3-10 from this standard shall be implemented on the internal network.	9-4
في حال كانت شبكة <اسم الجهة> تعمل على الإصدار الرابع من بروتوكول الإنترنت (IPv4)، يجب تثبيت ضوابط الأمن من المستوى 2 لحماية الشبكة الداخلية. In case <entity name> network is IPv4 based, Layer 2 security controls shall be deployed to protect the internal network	10-4
إعداد شبكات محلية افتراضية خاصة/معزولة لأجزاء الشبكة الحساسة أو الأجزاء المعزولة. Private/Isolated VLANs shall be configured for critical network segments or isolated segments.	11-4
منع إمكانية وصول الشبكات أو أجزاء الأنظمة الحساسة إلى أي نظام في البيئة ما لم يتم مسحها مع تطبيق الضوابط الأمنية المطلوبة والتحقق من الوضع الأمني للنظام. Networks or segments of critical systems shall not be allowed to access any system in the environment unless they are scanned, and if required security controls are applied and security posture of the system is verified.	12-4

13-4	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. Communications network shall be isolated by placing it in appropriate separate VLANs based on function and leveraging private VLANs or micro segmentation.
5	الوصول 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.
6	التشفير (Cryptography)
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 عالية نتيجة الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-6	وضع ضوابط على استخدام بروتوكولات الإدارة المشفرة الآمنة، مثل بروتوكول النقل الآمن (SSHv2) وبروتوكول التحكم بسطح المكتب عن بعد (RDP) عبر أمن طبقة النقل (TLS). The use of secure encrypted management protocols, such as Secure Shell (SSH) v2 and Remote Desktop Protocol (RDP) over TLS, shall be restricted.
2-6	تشفير حركة بيانات الشبكة السرية والمحمية باستخدام الجيل التالي من خوارزميات التشفير المدعومة (مثل التشفير بمجموعة "Suite B"). يُرجى الرجوع إلى معيار التشفير المعتمد في <اسم الجهة>. Sensitive and confidential network traffic shall be encrypted by using next generation encryption cipher suites (such as Suite B cryptography). Refer to <entity name>'s Cryptography Standard.
3-6	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"). يُرجى الرجوع إلى معيار التشفير المعتمد في <اسم الجهة>. Remote access traffic over IPSec or TLS shall be encrypted with next generation encryption cipher suites (such as Suite B

	cryptography). Refer to <entity name>'s Cryptography Standard.
4-6	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"). Application protocols shall be configured to use encryption wherever applicable (HTTPS, FTP over SSL, LDAP over SSL, etc.)
7	الأمن المادي (Physical Security)
الهدف	ضمان حماية جميع أجهزة الشبكة المطلوبة لاتصالات الشبكة من العبث أو التعديل أو أي هجمات مادية أخرى.
المخاطر المحتملة	يمكن أن يؤدي الهجوم المادي على أجهزة الشبكة 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	وضع كافة أجهزة الشبكة المطلوبة لاتصالات الشبكة في منطقة آمنة مع تطبيق ضوابط الوصول المادي عليها. All network devices that are required for network communications shall be placed in a secured area with physical access controls implemented.
2-7	وضع معدات الشبكة الرئيسية في منطقة محمية بنظام إنذار. Core network equipment shall be placed in an alarmed area.
3-7	ربط معدات الشبكة الرئيسية بمولد طاقة غير منقطعة (UPS) أو نظام توليد للطاقة. Core network equipment shall be attached to a UPS or a generator system.

4-7	إعداد آليات الدفاع المادية في أجهزة الشبكة، بما في ذلك آليات مثل: • الحماية عبر إعدادات نظام الإدخال/الإخراج الأساسي (BIOS). • نظام الإنذار بوجود محاولة لفتح هياكل الأجهزة. تمكين تلك الآليات في حال توفرها للتقنيات الموجودة. Physical defensive mechanisms shall be configured in network devices, including: • BIOS protection • Chassis intrusion alarm These mechanisms shall be enabled if available for the technologies in place.
8	التسجيل والمراقبة (Logging and Monitoring)
الهدف	ضمان مراقبة وتخزين كافة الأحداث الحساسة المتعلقة بأمن الشبكة من أجل الاكتشاف الاستباقي للهجمات السيبرانية وإدارة مخاطرها بفعالية لمنع أو تقليل الآثار المترتبة على أعمال <اسم الجهة>.
المخاطر المحتملة	لضمان سلامة الشبكة، 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 مما يؤدي إلى زيادة تكرار تلك الهجمات.
الإجراءات المطلوبة	
1-8	إعداد كافة أجهزة الأمن والشبكة 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 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 جميع أجهزة أمن الشبكة لتسجيل كافة طلبات شريط العنوان (URL) وكافة الجلسات المحجوبة وأحداث التهديدات. All network security devices shall be configured to log all URL requests, denied sessions and threat events.
4-8	إعداد أجهزة الشبكة لإرسال الأحداث المتعلقة بمحاولات الدخول الناجحة وغير الناجحة إلى واجهات الإدارة إلى نظام إدارة الأحداث والسجلات المركزي لأغراض التحليل والربط والتنبيه. 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.
5-8	تخزين كافة السجلات في بيئة آمنة مع تفعيل خاصية التحكم بالوصول إليها. All logs shall be stored in a secured environment with access control enabled.
9	الإعدادات والتحصين والنسخ الاحتياطية (Secure Configuration and Backup)
الهدف	ضمان أن أي تغييرات تنطوي على مخاطر كبيرة على شبكة <اسم الجهة> ستسير وفقاً لعملية الرقابة على التغيير.
المخاطر المحتملة	لضمان سلامة الشبكة، يجب عمل نسخ احتياطية من الإعدادات قبل تنفيذ أي تغييرات قد تعرض شبكة <اسم الجهة> إلى مخاطر كبيرة، كما يجب وضع سجل بالتغييرات لتتبعها وتحديد الجهات المسؤولة عنها.
الإجراءات المطلوبة	
1-9	صياغة الحد الأدنى من المعايير الأمنية الأساسية (MBSS) لكافة أجهزة الشبكة.

Minimum baseline security standards shall be developed for all network devices.	
مراجعة الحد الأدنى من المعايير الأمنية الأساسية (MBSS) بشكل منتظم لكافة الأجهزة مرة واحدة كل 6 أشهر على الأقل. Minimum baseline security standards shall be regularly reviewed for all devices at least every six months.	2-9
ضمان امتثال جميع الأجهزة بالحد الأدنى من المعايير الأمنية الأساسية (MBSS) والإبلاغ عن أي انحرافات يتم اكتشافها. All devices shall be compliant with the minimum baseline security standards, and any deviations discovered shall be reported.	3-9
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 A change control process shall be implemented and followed for any changes bearing a significant risk to <entity name>'s network, including rules that allow traffic to flow through network devices, firewall security policies, Network Address Translation (NAT), etc. The process shall be documented and shall include the following: • The rule's purpose	4-9

• The affected service(s) or application(s) • The affected users and devices • The date when the rule was added • The rule's expiration date, if applicable • The name of the person who added the rule • The problem statement • Supporting data • Management's approval of changes	
عمل نسخ احتياطية من الإعدادات لكافة معدات الشبكة المتضررة من التغيير قبل تطبيق التغيير على أرض الواقع. A backup of the configuration of all network equipment affected by a change shall be performed prior to the change implementation.	5-9
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.	6-9
إجراء التحديثات والإصلاحات على أجهزة الشبكات 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.	7-9
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.	8-9
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.	9-9

10	التحقق من سلامة البرمجيات والمعدات (Hardware and Software Integrity Validation)
الهدف	ضمان أن جميع برامج ومعدات 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 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 المادية بحثاً عن أي علامات لوجود عبث عند التركيب. All physical 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 من مصادر موثوقة. Software, updates, patches, and upgrades to network components shall be obtained from validated sources.
3-10	أثناء تنزيل البرمجيات من الإنترنت، يجب التحقق من التجزئة مع قاعدة بيانات المورد لكشف أي تعديل غير مصرح به على البرامج الثابتة أو البرمجيات. When downloading software from the Internet, hash verification shall be compared against the vendor's database to detect unauthorized modification to firmware or software.

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>.