الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

إرشادات الأمن السيبراني
لإنترنت الأشياء

Cybersecurity Guidelines for Internet of Things
(CGIoT-1: 2024)

إشارة المشاركة: أبيض

تصنيف الوثيقة: عام

إخلاء مسؤولية: تم إعداد الإرشادات الواردة في هذه الوثيقة بناءً على أفضل الممارسات في مجال الأمن السيبراني لإنترنت الأشياء، وهي إرشادات توعوية بهدف تقديم المعلومات فحسب. وتخلي الهيئة مسؤوليتها من أي تبعات قد تترتب بشكل مباشر أو غير مباشر على اتخاذ أي إجراءات؛ بناءً على المعلومات الواردة في هذه الوثيقة. وعند وجود تعارض بينَ ما ورد في هذه الوثيقة؛ مع أي متطلبات تشريعية أو تنظيمية؛ فإن تلك المتطلبات تحل محل ما ورد في هذه الوثيقة. وللحد من المخاطر المتعلّقة بالأمن السيبراني، والتخفيف من آثارها في الوقت المناسب؛ تحُث الهيئة الوطنية للأمن السيبراني جميع الجهات- إذا لم تكن مُلزمة وفق التشريعات ذات العلاقة -بإجراء تقييمات دورية لتلك المخاطر.

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

يستخدم هذا البروتوكول على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد، سواء أكان ذلك من داخل الجهة أم خارجها؛ خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب. ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

المستلم يمكنه مشاركة المعلومات مع آخرين في الجهة نفسها، أو جهة أخرى على علاقة معهم أو في القطاع نفسه؛ ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

قائمة المحتويات

قائمة الأشكال

قائمة الجداول

الملخص التنفيذي

قامت الهيئة الوطنية للأمن السيبراني بإعداد إرشادات الأمن السيبراني لإنترنت الأشياء (CGIoT-1:2024) التي يُوصى بتطبيقها في جميع الجهات المستخدمة لتقنية إنترنت الأشياء في المملكة؛ وذلك للحد من مخاطر الأمن السيبراني، المصاحبة للتبني الواسع النطاق لإنترنت الأشياء.

وتغطي هذه الإرشادات؛ أربع مكونات رئيسية، هي: حوكمة الأمن السيبراني، وتعزيز الأمن السيبراني، وصمود الأمن السيبراني، والأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية.

يُعنى مكون (حوكمة الأمن السيبراني) بضمان كون الإستراتيجية، والرؤية، وخارطة الطريق، والأهداف للجهة؛ تضع في الحسبان الأمن السيبراني لإ نترنت الأشياء. ويشمل ذلك الالتزام بالتنظيمات والتشريعات ذات العلاقة. ويُعنى هذا المكون كذلك؛ بتوثيق ونشر سياسات وإجراءات الأمن السيبراني ذات العلاقة بإنترنت الأشياء، بالإضافة إلى ضمان تحديد أدوار الأمن السيبراني ومسؤولياته لإنترنت الأشياء، لجميع الأطراف المعنية داخل الجهة، ضمن هيكلية الحوكمة. ويوضح هذا المكون أيضاً الإرشادات التي يوصى بتطبيقها فيما يخص إدارة مخاطر الأمن السيبراني لإنترنت الأشياء، ويضمن إدراج متطلبات الأمن السيبراني لإنترنت الأشياء، في دورة حياة إدارة المشاريع المعلوماتية والتقنية. بالإضافة إلى التركيز على جانب الأمن السيبراني لإنترنت الأشياء فيما يتعلق بالموارد البشرية، وتطوير برامج لتوعية وتدريب العاملين في مجال الأمن السيبراني المتعلق بإنترنت الأشياء.

فيما يخص مكون (تعزيز الأمن السيبراني)، فإنه يُعنى بضمان تطبيق آليات الأمن السيبراني الملائمة لمنظومة تقنية إنترنت الأشياء من أجل حماية المعلومات وأصولها ضد الهجمات السيبرانية. في حين يُعنى مكون (صمود الأمن السيبراني) بتعزيز قدرة الجهة على الصمود أمام الآثار التي قد تطرأ بسبب الحوادث المتعلقة بالأمن السيبراني لإنترنت الأشياء.

ويُعنى مكون (الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية) بتلبية الاحتياج للإدارة الفعالة لمخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية التي تعمل على دعم عمليات إنترنت الأشياء؛ بما في ذلك المخاطر المرتبطة بخدمات الحوسبة السحابية.

كما تحتوي هذه الوثيقة على مبادئ الأمن السيبراني لإنترنت الأشياء للمصنعين، والموضحة في ملحق (أ)، حيث يُوصى بتطبيقها من قبل الشركات المصنعة لتقنية إنترنت الأشياء، وذلك للحد من مخاطر الأمن السيبراني؛ في منتجات وخدمات إنترنت الأشياء.

المقدمة

مصطلح إنترنت الأشياء هو المعني بالحساسات والأجهزة ("الأشياء") المتصلة بالإنترنت و/أو الشبكات الأخرى، والتي تضيف قيمة، بناءً على البيانات؛ مثل تسهيل المهمات. وتدعم تقنية إنترنت الأشياء العديد من حالات الاستخدام بما في ذلك المنازل الذكية والمدن الذكية والرعاية الصحية الذكية والسيارات الذكية. ونظرًا للتبني الواسع لهذة التقنية؛ قد تكون الجهات المستخدمة لتقنية إنترنت الأشياء، أكثر عرضة للتهديدات والمخاطر السيبرانية.

وعلى هذا؛ قامت الهيئة الوطنية للأمن السيبراني، ويشار لها في هذه الوثيقة بـ (الهيئة) بإعداد إرشادات الأمن السيبراني لإنترنت الأشياء (CGIoT-1: 2024). وذلك بعد إجراء دراسة شاملة لعدة إرشادات، ومعايير، وأطر، وضوابط عالمية؛ تتعلق بالأمن السيبراني، و كذلك تحليل الوضع الراهن؛ والمتطلبات التشريعية، والتنظيمية في مجال تقنية إنترنت الأشياء في المملكة، وتحليل ماجرى رصده من الحوادث والهجمات السيبرانية السابقة، المتعلقة بإنترنت الأشياء. وتقدم وثيقة إرشادات الأمن السيبراني لإنترنت الأشياء (CGIoT– 1: 2024) ؛ إرشادات عامة فيما يخص تقنية إنترنت الأشياء، وعلى إنترنت الأشياء الصناعي، الالتزام بضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022).

تتكون إرشادات الأمن السيبراني لإنترنت الأشياء من:

- ٤ مكونات أساسية(Main Domains).
- ٢٧ مكونًا فرعيًا (Subdomains).
- ٨١ إرشادًا (Guidelines).

بالإضافة إلى ذلك؛ تحتوي الوثيقة على (١١) مبدءاً للأمن السيبراني لإنترنت الأشياء للمصنعين، مبين في الملحق (أ).

الأهداف

تهدف هذه الوثيقة إلى تقديم إرشادات غير مُلزمة، يكمن الغرض منها تضمين أفضل ممارسات الأمن السيبراني لدى الجهات التي تستخدم تقنية إنترنت الأشياء. وتستند هذه الممارسات إلى المعايير الرائدة مما يساعد الجهات عند تطبيقها على الحد من مخاطر الأمن السيبراني لإنترنت الأشياء التي تنشأ من التهديدات الداخلية والخارجية.

ومع تزايد الاعتماد على التقنيات المترابطة؛ قد تظهر مخاطر الأمن السيبراني المحتملة داخل منظومة إنترنت الأشياء. لذلك، يوصى بتضمين متطلبات الأمن السيبراني باستمرار في حوكمة إنترنت الأشياء، وتطويرها وصيانتها وإدارتها؛ لضمان حماية مصالح الجهات المعنية في هذه المنظومة.

وتأخذ هذه الإرشادات في الحسبان المحاور الأربعة الأساسية التي يرتكز عليها الأمن السيبراني، وهي:

- الاستراتيجية (Strategy)
- الأشخاص (People)
- الإجراء (Process)
- التقنية (Technology)

نطاق العمل وقابلية التطبيق

توصي الهيئة جميع الجهات التي تستخدم إنترنت الأشياء في المملكة، ويشار لها جميعًا في هذه الوثيقة باسم (الجهة)؛ باتباع هذه الإرشادات؛ لضمان تطبيق الحد الأدنى من أفضل الممارسات، والتقليل من مخاطر الأمن السيبراني، التي قد تنتج من استخدام هذه التقنية. كما تشجع الهيئة مصنّعي منتجات تقنية إنترنت الأشياء؛ على التقيد بالإرشادات الواردة في هذه الوثيقة، وكذلك مبادئ الأمن السيبراني لإنترنت الأشياء للمصّنعين (الواردة في الملحق (أ))عند تطوير منتجات وخدمات إنترنت الأشياء.

ونظرًا للطبيعة المتغيرة باستمرار للتهديدات السيبرانية؛ تحث الهيئة جميع الجهات والمصنعين على المراجعة الدورية، وتقييم المخاطر السيبرانية؛ لتحديد مدى الحاجة إلى اتخاذ تدابير إضافية فيما يتعلق بالأمن السيبراني لإنترنت الأشياء.

مكونات وهيكلية إرشادات الأمن السيبراني لإنترنت الأشياء

المكونات الأساسية والفرعية، لإرشادات الأمن السيبراني لإنترنت الأشياء

يوضح الشكل (١) أدناه، المكونات الأساسية والفرعية، لإرشادات الأمن السيبراني لإنترنت الأشياء

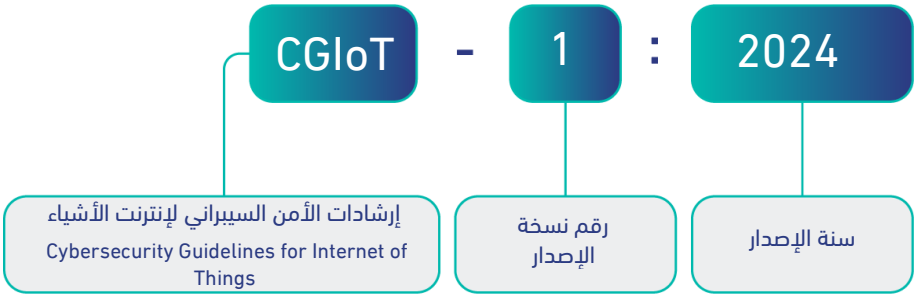
١ - حوكمة الأمن السيبرانى Cybersecurity Governance	١-١	استراتيجية الأمن السيبراني Cybersecurity Strategy	١-٢	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures
	١-٣	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities	١-٤	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management
	١-٥	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information and Technology Project Management	١-٦	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Compliance with Cybersecurity Standards, Laws and Regulations
	١-٧	المراجعة والتدقيق الدوري للأمن السيبراني Periodical Cybersecurity Review and Audit	١-٨	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources
	١-٩	برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program		
٢ - تعزيز الأمن السيبرانى Cybersecurity Defense	٢-١	إدارة الأصول Asset Management	٢-٢	إدارة هويات الدخول والصلاحيات Identity and Access Management
	٢-٣	حماية البريد الإلكتروني وأنظمة الرسائل الإلكترونية Email and Messaging Services Protection	٢-٤	إدارة أمن الشبكات Network Security Management
	٢-٥	أمن الأجهزة المحمولة المتصلة بإنترنت الأشياء IoT-Connected Mobile Device Security	٢-٦	حماية البيانات والمعلومات Data and Information Protection
	٢-٧	التشفير Cryptography	٢-٨	إدارة النسخ الاحتياطية Backup and Recovery Management

	٢-٩	إدارة الثغرات Vulnerability Management	٢-١٠	اختبار الاختراق Penetration Testing
	٢-١١	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	٢-١٢	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management
	٢-١٣	الأمن المادي Physical Security	٢-١٤	أمن تطبيقات إنترنت الأشياء IoT Application Security
	٢-١٥	إدارة دورة حياة أجهزة إنترنت الأشياء IoT Device Lifecycle Management		
٣. صمود الأمن السيبراني Cybersecurity Resilience	٣-١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience Aspects of Business Continuity Management (BCM)		
٤. الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third Party and Cloud Computing Cybersecurity	٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	٤-٢	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity

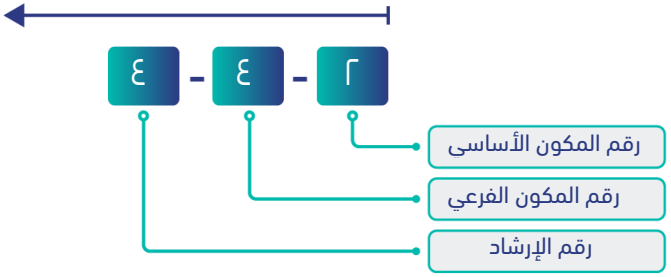
شكل ١:المكونات الأساسية والفرعية لإرشادات الأمن السيبراني لإنترنت الأشياء

الهيكلية

يوضح الشكلان (٢) و (٣) أدناه معنى رموز إرشادات الأمن السيبراني لإنترنت الأشياء:



شكل ٢ : معنى رموز إرشادات الأمن السيبراني لإنترنت الأشياء



شكل ٣ : هيكلية إرشادات الأمن السيبراني لإنترنت الأشياء

يوضح الجدول (١) أدناه طريقة هيكلية إرشادات الأمن السيبراني لإنترنت الأشياء.

1 رقم مرجعي للمكون الأساسي	اسم المكون الأساسي
رقم مرجعي للمكون الفرعي	اسم المكون الفرعي
الهدف	
الإرشادات	
رقم مرجعي للإرشاد	بنود الإرشاد

جدول ١ : هيكلية إرشادات الأمن السيبراني لإنترنت الأشياء

إرشادات الأمن السيبراني لإنترنت الأشياء

١ حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١	استراتيجية الأمن السيبراني
الهدف	ضمان احتواء الإستراتيجية والرؤية وخطط العمل والأهداف والمبادرات والمشاريع للأمن السيبراني في الجهة، على جوانب الأمن السيبراني الخاصة بإنترنت الأشياء، وإسهامها في تحقيق الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة.
الإرشادات	
١-١-١	تحديد متطلبات الأمن السيبراني لإنترنت الأشياء ضمن استراتيجية الأمن السيبراني الخاصة بالجهة وتوثيقها واعتمادها.
١-١-٢	تطوير خطة الأمن السيبراني لإنترنت الأشياء (ضمن خطة الأمن السيبراني العامة للجهة) وتوثيقها وتنفيذها، وتحديد الإجراءات والمبادرات ذات الأولوية لمعالجة مخاطر الأمن السيبراني ذات العلاقة بإنترنت الأشياء داخل الجهة.
١-١-٣	تحديد مؤشرات الأداء الرئيسة للأمن السيبراني لإنترنت الأشياء، ومتابعتها؛ لضمان تلبية متطلبات الأمن السيبراني طوال دورة حياة أجهزة إنترنت الأشياء.
١-١-٤	إجراء المراجعة الدورية على فترات زمنية مخطط لها، وإذا لزم الأمر؛ تحديث المبادرات والأهداف الإستراتيجية؛ أو عند حدوث تغيرات في المتطلبات التشريعية والتنظيمية المتعلقة بالأمن السيبراني لإنترنت الأشياء، بوضعه جزء من أعمال اللجنة الإشرافية لإدارة الأمن السيبراني في الجهة.
١-٢	سياسات وإجراءات الأمن السيبراني
الهدف	ضمان التوثيق والنشر لسياسات الأمن السيبراني لإنترنت الأشياء وإجراءته، والتزام الأطراف المعنيين داخل الجهة بها، وكذلك الأطراف الخارجية ذات العلاقة، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الإرشادات	
١-٢-١	تحديد سياسات وإجراءات الأمن السيبراني لإنترنت الأشياء وتوثيقها واعتمادها ونشرها، ضمن سياسات وإجراءات الأمن السيبراني العامة للجهة، مع الأطراف ذات العلاقة داخل الجهة وخارجها، بما في ذلك مع الموردين ومقدمي الخدمات من الأطراف الخارجية.
١-٢-٢	الحرص على دعم السياسات والإجراءات بمعايير تقنية أمنية على سبيل المثال لا الحصر (التحصينات / الحد الأدنى من معايير الأمان الأساسية للأنظمة المضمنة، ومعايير التحقق والصلاحيات للمستخدم، والشهادات الرقمية، ومعايير أمن تقسيم الشبكة، وما إلى ذلك).
١-٢-٣	إجراء المراجعة الدورية على فترات زمنية مخطط لها، وإذا لزم الأمر؛ تحديث السياسات والإجراءات والمعايير، وفقًا لمتطلبات الأعمال التنظيمية للجهة، أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣	أدوار ومسؤوليات الأمن السيبراني
الهدف	ضمان تحديد الأدوار والمسؤوليات لجميع الأطراف المعنية بالإدارة والتنفيذ والمراقبة لمتطلبات الأمن السيبراني لإنترنت الأشياء داخل الجهة.
الإرشادات	
١-٣-١	تحديد أدوار ومسؤوليات الأمن السيبراني لإنترنت الأشياء وتوثيقها واعتمادها ضمن الهيكل التنظيمي للحوكمة والأدوار والمسؤوليات ذات العلاقة بالأمن السيبراني للجهة، بحيث تتم معالجة متطلبات الأمن السيبراني وفقًا لسياسات وإجراءات الجهة.
١-٣-٢	إجراء المراجعة الدورية على فترات زمنية مخطط لها، وإذا لزم الأمر، تحديث أدوار ومسؤوليات الأمن السيبراني لإنترنت الأشياء، وفقًا لمتطلبات الأعمال التنظيمية للجهة، أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة.
١-٤	إدارة مخاطر الأمن السيبراني
الهدف	ضمان إدارة مخاطر الأمن السيبراني لإنترنت الأشياء على نحو ممنهج بهدف حماية أصول إنترنت الأشياء الخاصة بالجهة وفقًا للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الإرشادات	
١-٤-١	تحديد إجراءات إدارة مخاطر الأمن السيبراني لإنترنت الأشياء وتوثيقها واعتمادها وتنفيذها، وتحديد المخاطر وتقييمها والاستجابة لها ومتابعتها، بهدف تقليل تأثير التهديدات والهجمات المحتملة على بيئة إنترنت الأشياء، وتضمينها في منهجية وبرامج إدارة مخاطر الأمن السيبراني في الجهة.
١-٤-٢	تحديد قائمة بسيناريوهات مخاطر الأمن السيبراني الشائعة التي يمكن أن تؤثر على أجهزة إنترنت الأشياء وخدماتها أو المنظومة المرتبطة بها أو الجهة.
١-٤-٣	تحديد مخاطر الأمن السيبراني لإنترنت الأشياء وتوثيقها في سجل مخاطر الأمن السيبراني لإنترنت الأشياء ضمن السجل العام لمخاطر الأمن السيبراني للجهة.
١-٤-٤	إجراء تقييم مخاطر الأمن السيبراني لإنترنت الأشياء مع الأخذ في الحسبان التهديدات المحتملة لإنترنت الأشياء والسيناريوهات المحتملة للهجمات التي تستهدف أجهزة إنترنت الأشياء الشائعة واحتمالية تعطيل العمليات والأضرار المرتبطة بها.
١-٤-٥	تحديد مخاطر الأمن السيبراني لإنترنت الأشياء التي تتجاوز مستوى المخاطر المقبول وتحديد التدابير المناسبة لمعالجة هذه المخاطر وتقليل مستوى هذه المخاطر إلى المستوى المقبول في الجهة أو أقل منه.
١-٤-٦	إجراء المراجعة الدورية على فترات زمنية مخطط لها، وإذا لزم الأمر؛ تحديث إجراءات إدارة مخاطر الأمن السيبراني لإنترنت الأشياء، وفقًا للسياسات والإجراءات التنظيمية للجهة، أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة، وضمان مواءمتها مع متطلبات الأمن السيبراني لإنترنت الأشياء الخاصة بالجهة.
١-٥	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية
الهدف	ضمان شمول متطلبات الأمن السيبراني لإنترنت الأشياء في منهجية وإجراءات إدارة المشاريع بهدف حماية سرية وسلامة وتوافر أصول إنترنت الأشياء ومكوناتها وفقًا للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الإرشادات	
١-٥-١	تطبيق الممارسات الرائدة المتعلقة بمبادئ "الأمن من خلال التصميم" طوال مراحل دورة حياة تطوير أجهزة إنترنت الأشياء وخدماتها.
٢-٥-١	مراجعة أجهزة إنترنت الأشياء وخدماتها؛ لضمان مراعاتها لمتطلبات الأمن السيبراني، أثناء مراحل التخطيط والتصميم، للمشاريع المعلوماتية والتقنية.
٣-٥-١	تحديد إجراءات إدارة التغيير لإنترنت الأشياء لضمان التحكم في حالة الأمن السيبراني لإنترنت الأشياء في الجهة. ومنها: • مراعاة أنشطة إدارة التغيير عبر مراحل دورة حياة أنظمة إنترنت الأشياء، وأجهزتها، وخدماتها ، بما في ذلك مرحلة التطوير والتكامل، ومرحلة الصيانة أو التخلص، وكذلك أثناء التحديثات أو التصحيحات أو تغييرات الوظائف. • مراقبة التغيير ونشره إلى الأطراف ذات العلاقة داخل الجهة.
٦-١	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني
الهدف	ضمان توافق برامج الأمن السيبراني ومبادراته الخاصة بإنترنت الأشياء في الجهة؛ مع المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة.
الإرشادات	
١-٦-١	تطبيق آليات إنفاذ والتزام مناسبة لضمان توافق المتطلبات والبرامج والمبادرات والأنشطة التنظيمية، المتعلقة بإنترنت الأشياء، مع المتطلبات التشريعية والتنظيمية والمعايير المتعلقة بالأمن السيبراني.
٧-١	المراجعة والتدقيق الدوري للأمن السيبراني
الهدف	ضمان التأكد من أن متطلبات الأمن السيبراني لإنترنت الأشياء لدى الجهة مطبقة؛ وتعمل وفقًا للسياسات، والإجراءات التنظيمية للجهة؛ بالإضافة إلى المتطلبات التشريعية، والتنظيمية الوطنية، وغيرها.
الإرشادات	
١-٧-١	مراجعة تطبيق متطلبات الأمن السيبراني لإنترنت الأشياء، داخل الجهة، بشكل دوري، من قبل إدارة الأمن السيبراني.
٢-٧-١	المراجعة والتدقيق بشكل دوري، من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني، أو من قبل طرف خارجي، ضمن أعمال المراجعة والتدقيق الشاملة لمتطلبات الأمن السيبراني في الجهة، للتأكد من تطبيق متطلبات الأمن السيبراني لإنترنت الأشياء والالتزام بها وتوثيق نتائج عمليات التدقيق والمراجعة.
٣-٧-١	وضع إجراء وتطبيقه؛ لتسجيل أي حال بعدم الالتزام بمتطلبات الأمن السيبراني لإنترنت الأشياء، وإدارته؛ بالإضافة إلى تحديد الصلاحيات والمسؤوليات؛ لتنفيذ التوصيات والإجراءات التصحيحية لحالات عدم الالتزام، ورفع النتائج والتوصيات للمسؤولين واللجنة الإشرافية للأمن السيبراني.
٨-١	الأمن السيبراني المتعلق بالموارد البشرية
الهدف	ضمان التأكد من أن مخاطر الأمن السيبراني لإنترنت الأشياء المتعلقة بالعاملين (الموظفين والمتعاقدين) تعالج بفعالية خلال دورة حياتهم الوظيفية وفقًا للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الإرشادات	

١-٨-١	تحديد متطلبات الأمن السيبراني لإنترنت الأشياء للعاملين في الجهة قبل التوظيف وأثناء توظيف العاملين، وبعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة وتوثيقها واعتمادها وتنفيذها. ويشمل ذلك ما يلي: • التعريف بمتطلبات الأمن السيبراني، وتوثيق متطلبات التدريب المستمر للعاملين، مع التركيز بشكل خاص بمتطلبات الأمن السيبراني لإنترنت الأشياء. • تنفيذ متطلبات الأمن السيبراني لإنترنت الأشياء، والامتثال لها.
٢-٨-١	مراجعة صلاحيات وصول العاملين إلى أجهزة إنترنت الأشياء وخدماتها بشكل دوري، وتحديثها، أو إلغاؤها فوراً عند تغيير أدوار العاملين، أو إنهاء/انتهاء العلاقة الوظيفية، وفقًا لمبادئ التحكم بالدخول والصلاحيات (مبدأ الحاجة إلى المعرفة والاستخدام، ومبدأ الحد الأدنى من الصلاحيات والامتيازات، ومبدأ فصل المهام).
٣-٨-١	إجراء المراجعة الدورية على فترات زمنية مخطط لها، وإذا لزم الأمر؛ تحديث متطلبات الأمن السيبراني لإنترنت الأشياء للعاملين في الجهة، وفقًا للسياسات والإجراءات التنظيمية للجهة، أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة.
٩-١	برنامج التوعية والتدريب بالأمن السيبراني
الهدف	ضمان التأكد من أن العاملين يتم توعيتهم بجوانب الأمن السيبراني ذات العلاقة بإنترنت الأشياء، وكذلك التأكد من تزويد العاملين في الجهة بالمهارات والمؤهلات، والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية أصول إنترنت الأشياء الخاصة بالجهة، والقيام بمسؤولياتهم تجاه الأمن السيبراني لإنترنت الأشياء.
الإرشادات	
١-٩-١	تضمين جوانب الأمن السيبراني لإنترنت الأشياء، ضمن برنامج التوعية بالأمن السيبراني واستراتيجية التدريب داخل الجهة. ويشمل ذلك على ما يلي: • تحديد استراتيجية تدريب العاملين ذوي المهامات الوظيفية المتعلقة بإنترنت الأشياء؛ وتوثيقها واعتمادها. • تدريب العاملين على أفضل ممارسات الأمن السيبراني من أجل ضمان الاستخدام الآمن لأجهزة إنترنت الأشياء وخدماتها. • تضمين البرامج التدريبية بأفضل الممارسات المطبقة، ومهمات الأمن السيبراني لإنترنت الأشياء ومسؤولياته، والسياسات والمعايير؛ لضمان بيئة عمل آمنة.
٢-٩-١	تعزيز الوعي بالأمن السيبراني لإنترنت الأشياء، على جميع مستويات الجهة؛ مع مراعاة الآتي: • توعية العاملين في جميع مستويات الجهة بأهمية حماية أجهزة إنترنت الأشياء؛ بما في ذلك صناع القرار. • تنفيذ أنشطة التوعية بالأمن السيبراني؛ لزيادة الوعي بالأمن السيبراني لإنترنت الأشياء بين العاملين؛ من خلال الدورات التدريبية، وأنشطة محاكاة حوادث الأمن السيبراني المتعلقة بإنترنت الأشياء، وكتيبات أفضل ممارسات الأمن السيبراني ذات العلاقة بإنترنت الأشياء، وعبر البريد الإلكتروني، وخلال الاجتماعات وغيرها من طرق التوعية وقنواتها. • تقييم مهارات الأمن السيبراني في إنترنت الأشياء للعاملين عليها؛ من أجل تحديد الفجوات المعرفية، وتخطيط التدريب، بناءً على المهارات المطلوبة لكل وظيفة. • ضمان أن العاملين الذين يستخدمون أجهزة إنترنت الأشياء وخدماتها، على اطلاع مستمر، بأحدث التطورات في مجال الأمن السيبراني لإنترنت الأشياء.

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-١	إدارة الأصول
الهدف	ضمان امتلاك الجهة، لقائمة جرد دقيقة، ومفصلة، وحديثة لجميع الأصول ذات العلاقة بإنترنت الأشياء من أجل الحفاظ على سرية أجهزة إنترنت الأشياء، وسلامتها، وتوافرها، بما يتسق مع متطلبات الأمن السيبراني والعمليات التشغيلية في الجهة.
الإرشادات	
٢-١-١	الاحتفاظ بقائمة جرد لجميع الأصول ذات العلاقة بأجهزة إنترنت الأشياء وخدماتها التي تستخدمها الجهة، بحيث تشتمل على التسمية، والتصنيف، والحساسية، والمكونات، وقدرات الأجهزة والبرمجيات، بما في ذلك التابعة للأطراف الخارجية. إذ تختلف قدرات أجهزة إنترنت الأشياء باختلاف أنواعها، وهو ما قد يعرّض بيئة إنترنت الأشياء في الجهة للمخاطر المختلفة.
٢-١-٢	إجراء المراجعات الدورية لقائمة جرد أصول إنترنت الأشياء ومتابعة جميع التغييرات داخل الجهة.
٢-٢	إدارة هويات الدخول والصلاحيات
الهدف	منع الوصول غير المصرح به إلى أصول إنترنت الأشياء، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة.
الإرشادات	
٢-٢-١	إدارة هويات الدخول وصلاحياتها، إلى أصول إنترنت الأشياء، وتقييد الوصول إلى بياناتها وأجهزتها وخدماتها على المستخدمين المصرح لهم فحسب، بناءً على مبادئ التحكم بالدخول والصلاحيات (مبدأ الحاجة إلى المعرفة والاستخدام، ومبدأ الحد الأدنى من الصلاحيات والامتيازات، ومبدأ فصل المهام). بالإضافة إلى إدارة الحسابات ذات الصلاحيات الهامة والحساسة على أجهزة إنترنت الأشياء وخدماتها.
٢-٢-٢	تطبيق معايير عالية، للتحقق من الهوية، للوصول إلى أجهزة إنترنت الأشياء وخدماتها، واتباع أفضل الممارسات على سبيل المثال لا الحصر: ● إلزام المستخدمين، بعدم استخدام كلمات المرور، الثابتة والافتراضية. ● إلزام المستخدمين بتغيير كلمات المرور بشكل دوري. ● زيادة تعقيد كلمات المرور؛ مثل تحديد الحد الأدنى لطول الكلمة، واستخدام مجموعة من الأحرف (الأحرف الكبيرة والصغيرة) والأرقام والرموز. ● تطبيق تدابير لمنع عرض كلمة مرور المستخدم على واجهات تسجيل الدخول في التطبيقات. ● وضع حد أقصى لمحاولات الدخول الخاطئة. ● تفعيل التقنيات الآمنة للتحقق من الهوية ، ما أمكن ذلك.
٢-٢-٣	إجراء المراجعات لهويات الدخول والصلاحيات إلى أصول إنترنت الأشياء؛ بناءً على مبادئ التحكم بالدخول والصلاحيات.
٢-٣	حماية البريد الإلكتروني وأنظمة الرسائل الإلكترونية

الهدف	ضمان تنفيذ متطلبات الأمن السيبراني لحماية بيانات إنترنت الأشياء عبر البريد الإلكتروني وخدمات المراسلة الأخرى مثل الرسائل النصية القصيرة، لحماية تلك البيانات من المخاطر السيبرانية.
الإرشادات	
٢-٣-١	تحديد متطلبات الأمن السيبراني لحماية البيانات المنقولة بين أجهزة إنترنت الأشياء/خدماتها، وخدمات البريد الإلكتروني والرسائل بالجهة وتوثيقها واعتمادها ومراجعتها دورياً.
٢-٣-٢	تطبيق متطلبات الأمن السيبراني لحماية البيانات المنقولة بين أجهزة إنترنت الأشياء/خدماتها، وخدمات البريد الإلكتروني والرسائل بالجهة، ضمن إجراءات حماية خدمات البريد الإلكتروني والرسائل للجهة.
٢-٤	إدارة أمن الشبكات
الهدف	تطوير قدرات اتصال، وتكامل آمنة وموثوقة، بين أجهزة إنترنت الأشياء المختلفة في الشبكة.
الإرشادات	
٢-٤-١	تحديد متطلبات الأمن السيبراني للاتصال الآمن بين أجهزة إنترنت الأشياء/خدماتها ، وبيئة الاستخدام بما في ذلك الأجهزة الأخرى والبنية التحتية التقنية/السحابية وتوثيقها، واعتمادها، وتطبيقها، ومراجعتها دورياً.
٢-٤-٢	تطبيق تدابير لتأمين اتصال البيانات بين الأجهزة المختلفة المتصلة في الشبكة، بما في ذلك مصادقة أجهزة إنترنت الأشياء الأخرى (الأجهزة النظيرة "Peer Devices") التي تحاول الإتصال بها.
٢-٤-٣	تشفير عمليات انتقال البيانات بين أجهزة إنترنت الأشياء وخدماتها، والمصادقة عليها؛ بالإضافة إلى تأمين البنية التحتية الأساسية، ما أمكن ذلك.
٢-٤-٤	تطبيق العزل والتقسيم المنطقي و/ أو المادي بين بيئة إنترنت الأشياء، وبيئة الجهة، بناءً على دراسة المخاطر السيبرانية لدى الجهة، ما أمكن ذلك.
٢-٤-٥	وضع البوابات الأمنية (Security Gateway) على أجهزة إنترنت الأشياء وخدماتها الخارجية (Internet- Facing IoT devices and services) لتأمين الاتصال والتواصل بينها وبين الإنترنت.
٢-٤-٦	استخدام خوادم التحديث الآمنة، لضمان النقل الآمن لملفات التحديث الخاصة ببرمجيات/البرامج الثابتة لجهاز إنترنت الأشياء، وإعداداته، وتطبيقاته، مع ضمان ووضع آليات مصادقة وتشفير مناسبة، لنقل التحديثات.
٢-٥	أمن الأجهزة المحمولة المتصلة بإنترنت الأشياء
الهدف	ضمان تطبيق متطلبات الأمن السيبراني للأجهزة المحمولة (على سبيل المثال لا الحصر: الهواتف الذكية والأجهزة الذكية المحمولة)، المتصلة بأجهزة إنترنت الأشياء وخدماتها؛ لتعزيز حمايتها، وتقليل مخاطر الأمن السيبراني فيها.
الإرشادات	
٢-٥-١	تطبيق التدابير الآتية للأجهزة المحمولة المتصلة بإنترنت الأشياء: • تنفيذ تدابير لتأمين الاتصال بين جهاز إنترنت الأشياء، والأجهزة المحمولة. • تقييد الوصول إلى الأجهزة المحمولة المتصلة بإنترنت الأشياء، على المستخدمين المصرح لهم فحسب. • استخدام طرق المصادقة الآمنة، للوصول إلى بيانات الجهاز المحمول، وجهاز إنترنت الأشياء. • تنفيذ الممارسات الآمنة، عند تطوير البرمجيات، لتطبيقات الأجهزة المحمولة، التي تتفاعل مع أجهزة إنترنت الأشياء.

	• الحذف الآمن لبيانات أجهزة إنترنت الأشياء، المخزنة على الأجهزة المحمولة؛ عند فقدان تلك الأجهزة المحمولة، أو عند انتهاء الحاجة إلى استخدامها.
٦-٢	حماية البيانات والمعلومات
الهدف	ضمان سرية البيانات التي تتم معالجتها بواسطة أجهزة إنترنت الأشياء وخدماتها، وكذلك ضمان سلامتها وتوافرها.
الإرشادات	
١-٦-٢	تطبيق آليات لتصنيف البيانات الخاصة بأجهزة إنترنت الأشياء/خدماتها وترميزها؛ حسب التشريعات والتنظيمات ذات العلاقة، والمتطلبات التنظيمية في الجهة.
٢-٦-٢	تطبيق تدابير الحماية؛ لتجنب الوصول غير المصرح به إلى البيانات المتعلقة بإنترنت الأشياء، أو العبث بها عند تخزينها، أو أثناء نقلها.
٣-٦-٢	منع أجهزة إنترنت الأشياء وخدماتها من جمع البيانات الحساسة غير المطلوبة أو التي لا يمكن حمايتها بشكلٍ كافٍ.
٧-٢	التشفير
الهدف	ضمان الاستخدام المناسب للتشفير بهدف تأمين عمليات إنتقال البيانات، وتبادلها بين أجهزة إنترنت الأشياء.
الإرشادات	
١-٧-٢	تحديد متطلبات الأمن السيبراني لإنترنت الأشياء فيما يخص تشفير بيانات إنترنت الأشياء، وفقًا للمعايير الوطنية للتشفير (NCS-1:2020) وتوثيقها، واعتمادها، وتطبيقها، ومراجعتها دوريًا.
٢-٧-٢	تشفير البيانات، سواء أكان ذلك أثناء التخزين، أو أثناء النقل، ما أمكن ذلك.
٨-٢	إدارة النسخ الاحتياطية
الهدف	ضمان تطبيق النسخ الاحتياطي، واستعادة البيانات لأجهزة إنترنت الأشياء وخدماتها؛ وذلك بهدف حماية البيانات التي تتم معالجتها بواسطة هذه الأجهزة من الأضرار الناجمة عن المخاطر السيبرانية.
الإرشادات	
١-٨-٢	تحديد متطلبات الأمن السيبراني لإنترنت الأشياء لإدارة النسخ الاحتياطية واستعادة عمل الأنظمة والبيانات، ضمن سياسات إدارة النسخ الاحتياطية والاستعادة في الجهة وتوثيقها، واعتمادها، وتطبيقها، ومراجعتها دوريًا.
٢-٨-٢	ضمان توفر نسخ مخزنة محليًا لبيانات وبرمجيات إنترنت الأشياء، تم اختبارها والتحقق من موثوقيتها، للتمكن من استعادة البيانات بشكل آمن.
٣-٨-٢	إجراء المراجعات الدورية للنسخ الاحتياطية المخزنة لأجهزة إنترنت الأشياء واختبارها.
٩-٢	إدارة الثغرات
الهدف	ضمان اكتشاف الثغرات الأمنية في الوقت المناسب، ومعالجتها بشكل فعال، وذلك لمنع احتمالية استغلالها في شن الهجمات السيبرانية على الجهة.
الإرشادات	
١-٩-٢	فحص واكتشاف ثغرات الأمن السيبراني ومراقبتها باستمرار ومعالجتها في أجهزة إنترنت الأشياء وخدماتها.

٢-٩-٢	تنصيب التحديثات والإصلاحات على جميع مكونات البرمجيات/البرامج الثابتة، ضمن أجهزة إنترنت الأشياء في الوقت المناسب حسب الآتي: ● تنفيذ تصحيحات البرمجيات بطريقة وقائية؛ لضمان الحد من ثغرات الأمن السيبراني، قبل أن يتم استغلالها. ● ضمان أن جهاز إنترنت الأشياء يحافظ على الوظائف الأساسية، أثناء تنصيب التحديثات والإصلاحات. ● استخدام أحدث نظم التشغيل، عند تطوير أجهزة إنترنت الأشياء، مما يساعد في ضمان أن الثغرات المعروفة قد تمت معالجتها.
١٠-٢	اختبار الاختراق
الهدف	تقييم كفاءة الأمن السيبراني لإنترنت الأشياء وتعزيز قدراته داخل الجهة؛ من خلال القيام بمحاكاة الهجمات السيبرانية لتحديد نقاط الضعف غير المعروفة، التي قد تؤدي إلى اختراقات سيبرانية.
الإرشادات	
١-١٠-٢	تنفيذ عمليات اختبار الاختراق؛ من أجل اكتشاف الثغرات استباقيًا في برمجيات إنترنت الأشياء ومكوناتها، وذلك عن طريق الآتي: ● تحديد أصول إنترنت الأشياء ضمن نطاق عمل اختبار الاختراق وتحليلها. ● التحقق من الثغرات المعروفة واختبار قابلية استغلالها؛ إلى جانب الكشف عن الثغرات الغير معروفة (Zero-Day Vulnerabilities) في أجهزة إنترنت الأشياء وخدماتها. ● تحديد الإعدادات غير الآمنة وتقييمها على مستوى التطبيق، والشبكة، والبيانات و/أو على مستوى الحساسات، و/أو بوابة الجهاز. ● تطوير و تطبيق الإجراءات المناسبة للإبلاغ والتحذير؛ من أجل القدرة على ترتيب أولويات اتخاذ القرارات المتعلقة بكيفية تضمين تدابير الأمن السيبراني الإضافية.
٢-١٠-٢	تنفيذ تمارين فريق اختبار الكفاءات الدفاعية؛ وذلك باستهداف أجهزة إنترنت الأشياء وخدماتها ذات المهمات الحساسة، كمحاكاة هجمات الهندسة الاجتماعية، والوصول المادي غير المصرح به، والاختراق، وغيرها من التقنيات الخادعة، التي تهدف إلى الوصول غير المصرح به إلى المعلومات، والأصول الحساسة، ما أمكن ذلك.
١١-٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني
الهدف	ضمان جمع سجلات أحداث الأمن السيبراني وحالات التهديد لإنترنت الأشياء ومراقبتها، وتحليلها، على نحو منتظم، وذلك بهدف الكشف المبكر عن أي هجمات سيبرانية محتملة على أجهزة إنترنت الأشياء وخدماتها.
الإرشادات	
١-١١-٢	ضمان أن أجهزة إنترنت الأشياء لديها القدرة على تسجيل أحداث الأمن السيبراني، وتخزين البيانات مركزيًا لمراقبتها من قبل مركز عمليات الأمن السيبراني (SOC) في الجهة، ما أمكن ذلك. مع مراعاة الآتي: ● تحديد السيناريوهات لاكتشاف حوادث الأمن السيبراني المحتملة لإنترنت الأشياء.

	• تسجيل الأحداث مثل التحقق من هوية المستخدمين، وإدارة الحسابات، وصلاحيات الوصول، ومحاولات الوصول إلى البيانات الحساسة، والتعديلات على موارد النظام. • مراقبة سجلات الأحداث والتهديدات لإنترنت الأشياء ومراجعتها وتحليلها على نحو منتظم، وتنفيذ أنظمة آلية؛ لتمكين المراقبة المباشرة للسجلات والتهديدات؛ إن أمكن. • تفعيل خدمة تخزين السجلات في مخازن بيانات عن بعد، بدلًا من تخزينها محليًا، بحيث تظل بيانات السجلات آمنة، حتى في حال اختراق برمجيات ومكونات الأجهزة. وتنفيذ آليات التحقق من الهوية للوصول إلى مخازن البيانات لتمكين الاستعادة الآمنة لبيانات السجلات. • عند رصد تغيير أو سلوك غير مصرح به في جهاز إنترنت الأشياء؛ فإنه يلزم القيام بتنبيه المستهلك و/أو المسؤول، مع التأكد من كون الجهاز لا يتصل بشبكة أوسع مما هو ضروري؛ لتمكين إرسال التنبيه. • تحليل سوء الاستخدام المحتمل لصلاحيات الوصول من قبل الأطراف المعنية داخليًا. • فحص بيانات القياس عن بُعد (Telemetry Data) التي تم جمعها بواسطة أجهزة إنترنت الأشياء وخدماتها؛ مثل بيانات الاستخدام، والقياس، والسجلات، لاكتشاف الحالات المشبوهة، وتحديد الظروف غير العادية في الوقت المناسب. • تحديد فترة الاحتفاظ ببيانات أحداث الأمن السيبراني؛ بمدة لاتقل عن ١٢ شهرًا على الأقل من تاريخ تسجيلها.
٢-١١-٢	فحص المعلومات التشخيصية بانتظام لأجهزة إنترنت الأشياء؛ لتشتمل على تفاصيل؛ مثل بيانات درجة الحرارة، وبيانات استخدام الذاكرة، وعمر البطارية، وبيانات تنفيذ العمليات، للتمكن من رصد أي حادث محتمل للأمن السيبراني بشكل أفضل.
٢-١٢	إدارة حوادث وتهديدات الأمن السيبراني
الهدف	ضمان تحديد التهديدات وحوادث الأمن السيبراني لإنترنت الأشياء ومعالجتها في الوقت المناسب، من أجل تقليل التأثير السلبي على العمليات في الجهة.
الإرشادات	
٢-١٢-١	تضمين نموذج إدارة الحوادث، والتهديدات الخاصة بإنترنت الأشياء، ضمن أنشطة إدارة حوادث وتهديدات الأمن السيبراني وبرامجها للجهة.
٢-١٢-٢	وضع خطة لإدارة حوادث الأمن السيبراني لإنترنت الأشياء؛ لتشمل الاستجابة للحوادث، وإجراءات المعالجة بما يتسق مع ممارسات إدارة الحوادث للجهة؛ ومنها: • الاستعداد للحوادث؛ من خلال التأكد من كون الأنظمة والشبكات والتطبيقات آمنة. • كشف الحوادث وتحليلها وتوثيقها. • إبلاغ الأطراف المعنية عن الحوادث ومنها الهيئة الوطنية للأمن السيبراني. • احتواء الحوادث، ومعالجتها، والتعافي من آثارها. • إعداد تقارير متابعة عن الحوادث.

٢-١٢-٣	تطوير قدرات إجراء التحليلات اللازمة، بعد كل حادث؛ للكشف عن عناصر البرمجيات والأجهزة والمكونات لأجهزة إنترنت الأشياء التي تأثرت بهذه الحوادث بالتحديد، وتقييمها، واستخدام هذا التحليل لتوفير تحديثات الأمن السيبراني الضرورية، أو القيام باستدعاء الأجهزة (حسب قابلية التطبيق) لتنفيذ تحديثات الأمن السيبراني الضرورية، مثل ترقية البرامج الثابتة القديمة، التي تحتوي على كلمات مرور افتراضية.
٢-١٢-٤	تحديد متطلبات الأمن السيبراني لإنترنت الأشياء لإدارة التهديدات ضمن عملية نمذجة التهديدات السيبرانية التي طورتها الجهة وتوثيقها واعتمادها، وتطبيق الممارسات الآتية ضمن خطة إدارة تهديدات الأمن السيبراني لإنترنت الأشياء: ● تتبع المعلومات الاستباقية المستخلصة من استخدام أجهزة إنترنت الأشياء وخدماتها، ومراقبتها وتوثيقها. ● مشاركة المعلومات المتعلقة بمؤشرات الاختراقات؛ والمعلومات الاستباقية مع الهيئة الوطنية للأمن السيبراني. ● مراجعة متطلبات الأمن السيبراني لإنترنت الأشياء لإدارة التهديدات دورياً.
٢-١٣	الأمن المادي
الهدف	ضمان حماية أصول إنترنت الأشياء، من الوصول المادي غير المصرح به؛ وكذلك الحماية من الفقد والسرقة والتلف.
الإرشادات	
٢-١٣-١	تطبيق أنظمة الكشف المادي (Physical Detection Systems) لمراقبة مناطق العمل الحساسة، ذات العلاقة بأجهزة إنترنت الأشياء وخدماتها، والتي يمكن أن تشمل غرف الخوادم، أو مناطق العمل الأخرى المخصصة لإدارة شبكة الجهة، أو الاتصال الخارجي، أو الخدمات الخارجية؛ مثل خدمة الحوسبة السحابية والإنترنت والمراقبة.
٢-١٣-٢	تنفيذ التدابير اللازمة؛ لحماية أجهزة إنترنت الأشياء، من محاولات العبث المادي، بها ورصد تلك المحاولات.
٢-١٤	أمن تطبيقات إنترنت الأشياء
الهدف	ضمان أمان تطبيقات البرامج التي تعمل على أجهزة إنترنت الأشياء وكذلك ضمان موثوقيتها.
الإرشادات	
٢-١٤-١	تنفيذ تدابير الأمن السيبراني التقنية؛ لتأمين واجهات تطبيقات إنترنت الأشياء، للحد من الكشف عن البيانات، والإعدادات، وعمليات الإدارة، ومنع الوصول غير المصرح به.
٢-١٤-٢	تطبيق إجراءات؛ للسماح بقائمة محددة من التطبيقات (Application Whitelisting) من العمل على نظام تشغيل جهاز إنترنت الأشياء وذلك للمساعدة في منع البرمجيات الضارة، والتطبيقات غير المصرح بها، من العمل على نظام التشغيل؛ بما في ذلك تطبيقات الجهات الخارجية، غير الموثوق بها.
٢-١٤-٣	تنفيذ ممارسات التطوير البرمجية الآمنة؛ لتطبيقات إنترنت الأشياء، ومراجعة الشفرة المصدرية، لتلافي الأخطاء البرمجية ذات التأثير على الأمن السيبراني أو الحد منها.
٢-١٤-٤	تحديث قائمة التطبيقات المسموح بها، بشكل دوري؛ لتشمل التطبيقات والوظائف، والتحديثات والإصلاحات للبرمجيات.
٢-١٥	إدارة دورة حياة أجهزة إنترنت الأشياء
الهدف	ضمان التثبيت والإعداد الآمن لأجهزة إنترنت الأشياء، وإيجاد خطط سحب واستبدال للأجهزة.

الإرشادات	
٢-١٥-١	استخدام الأجهزة التي تتضمن وظائف الأمن السيبراني على مستوى المكونات؛ للحفاظ على حماية الأجهزة وسلامتها، مع اتباع المتطلبات التالية لتأمين مكونات الأجهزة: ● نشر مكون جذر الثقة (Root of Trust) في الأجهزة، من أجل المساعدة في التحقق من صحة المكونات والبرامج الثابتة والبرمجيات قبل تحميلها؛ من أجل بناء الثقة في بيئة التمهيد. ● حصر استخدام منافذ أجهزة إنترنت الأشياء الخارجية، على المنافذ الضرورية فحسب، لعمل الجهاز وضمان موثوقية الأجهزة المتصلة بها.
٢-١٥-٢	تحديد خطوات تثبيت أجهزة إنترنت الأشياء وخدماتها، وإعدادها. ويُنصح أن تتوافق هذه الخطوات مع أفضل ممارسات الأمن السيبراني، فيما يتعلق بإمكانية استخدام الأجهزة و الخدمات، وتشمل على سبيل المثال لا الحصر: ● تطبيق الإعدادات الآمنة وخيارات التحصينات التي تنطبق على الجهة، مثل تعطيل سمات، أو وظائف معينة، لن تستخدمها الجهة. ● تجهيز أجهزة إنترنت الأشياء واعدادها بطريقة آمنة، للحد من التعرض إلى التهديدات، مثل ضمان كون جميع الأجهزة والتطبيقات/الخدمات المرتبطة بها؛ لا تحتوي على كلمة مرور افتراضية، وأن تكون كلمات المرور فريدة ومعقدة. ● تنفيذ اختبارات الأمن السيبراني؛ قبل نشر التطبيق في بيئة الإنتاج. ● إجراء اختبارات الأمن السيبراني بشكل دوري؛ قبل كل إصدار جديد للبرمجيات وبعده.
٢-١٥-٣	وضع خطة معنية بسحب أجهزة إنترنت الأشياء وخدماتها في نهاية دورة حياتها. بالإضافة إلى تنفيذ الممارسات الآتية لوضع استراتيجية عند نهاية العمر الافتراضي لأجهزة إنترنت الأشياء وخدماتها: ● وضع خطة استبدال، وخطة نهاية العمر الافتراضي لأجهزة إنترنت الأشياء وخدماتها، التي انتهى الدعم الخاص بها و/أو لم تعد تدعم وظائف الأمن السيبراني الأساسية. بالإضافة إلى تضمين مكونات الأطراف الخارجية في خطة نهاية العمر الافتراضي للأجهزة والخدمات. ● تنفيذ تدابير لإتلاف البيانات التي تم تخزينها، أو معالجتها، بواسطة جهاز/خدمة إنترنت الأشياء، وفقًا للتشريعات والتنظيمات ذات العلاقة في الجهة. ● الاحتفاظ بسجل تدقيق لمراقبة عملية التخلص من أجهزة إنترنت الأشياء وخدماتها.

٣ صمود الأمن السيبراني(Cybersecurity Resilience)

٣-١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال
الهدف	ضمان توافر متطلبات صمود الأمن السيبراني لإنترنت الأشياء ضمن خطة إدارة استمرارية الأعمال للجهة، وذلك من أجل تعزيز سلامة أجهزة إنترنت الأشياء وخدماتها أثناء حوادث الأمن السيبراني.
الإرشادات	
٣-١-١	تحديد وتوثيق واعتماد متطلبات صمود الأمن السيبراني في الحفاظ على سرية أجهزة إنترنت الأشياء والمكونات المرتبطة بها وسلامتها وتوافرها؛ ضمن إدارة استمرارية الأعمال للجهة، ومراجعتها دورياً. وتنفيذ الممارسات الآتية: ● تطوير متطلبات الصمود مع الأخذ بعين الاعتبار مدى تأثير تعطل الوظائف الأساسية لأجهزة إنترنت الأشياء بسبب الهجمات السيبرانية على إجراءات الأعمال المرتبطة بها. ● تطبيق تدابير الصمود اللازمة، التي تتناسب مع الاستخدام المقصود لكل جهاز؛ مع مراعاة المكونات الأخرى المرتبطة بنظام إنترنت الأشياء، أو الخدمة أو الجهاز. ● ضمان أن وظائف الأمن السيبراني الأساسية لأجهزة إنترنت الأشياء وخدماتها؛ قادرة على العمل محلياً، في حال انقطاع التيار أو الشبكة، ولها القدرة على العودة إلى الحالة المطلوبة بعد الانقطاع.
٣-١-٢	على الأجهزة الطرفية، وخاصة أجهزة البوابة لإنترنت الأشياء؛ أن تكون قادرة على تطبيق متطلبات الأمن السيبراني، عبر شبكات وبروتوكولات الاتصال حتى في حال انقطاع/تعطيل الاتصال بالشبكة الرئيسية، ما أمكن ذلك.

٤ الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity)

٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية
الهدف	ضمان حماية أصول الجهة من مخاطر الأمن السيبراني في أجهزة إنترنت الأشياء، التي يتم شراؤها أو تشغيلها من قبل أطراف خارجية.
الإرشادات	
٤-١-١	تحديد متطلبات الأمن السيبراني لإنترنت الأشياء ضمن العقود مع الموردين والأطراف الخارجية، وتوثيقها واعتمادها وتطبيقها ومراجعتها دوريًا.
٤-١-٢	الطلب من المصنعين، ومقدمي الخدمات لمنتجات إنترنت الأشياء وخدماتها، إثبات قدرات الأمن السيبراني في منتجاتهم و/أو خدماتهم، و تطبيق مبادئ "الأمن من خلال التصميم" طوال مراحل دورة حياة تطوير أجهزة/خدمات إنترنت الأشياء.
٤-١-٣	الطلب من المطورين والمصنعين، تقديم قائمة بمكونات الأجهزة، والبرمجيات الموجودة في أجهزة إنترنت الأشياء وخدماتها؛ لمساعدة الجهة في فهم مخاطر الأمن السيبراني وإدارتها بشكل أفضل وتصحيح أي ثغرات أمنية معروفة.
٤-١-٤	تحديد أنظمة المعلومات، والمكونات، والخدمات، ذات العلاقة بإنترنت الأشياء المقدمة من قبل الموردين والأطراف الخارجية لإدراجها في التقييم العام للمخاطر، وإجراءات التقليل من المخاطر.
٤-١-٥	تنفيذ أنشطة التحقق من خلال عمليات التدقيق، والاختبارات، والتحقق من شهادات البرمجيات؛ لضمان أن جميع المكونات المقدمة من الأطراف الخارجية في أجهزة إنترنت الأشياء؛ متوافقة مع سياسات الأمن السيبراني للجهة والمتطلبات الموضحة في العقود.
٤-١-٦	مراجعة إجراءات معالجة مخاطر الأمن السيبراني، ومتطلبات الأمن السيبراني لإنترنت الأشياء ذات العلاقة بالموردين والأطراف الخارجية؛ لرصد أي إجراء غير مصرح به.
٤-٢	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة
الهدف	ضمان تنفيذ متطلبات الأمن السيبراني لخدمات الحوسبة السحابية المستخدمة في أجهزة إنترنت الأشياء.
الإرشادات	
٤-٢-١	تحديد متطلبات الأمن السيبراني لخدمات الحوسبة السحابية التي تستضيف خدمات إنترنت الأشياء والعمل على توثيقها واعتمادها وتطبيقها، بالإضافة إلى خدمات الحوسبة السحابية الأخرى المستخدمة خصيصًا لأجهزة إنترنت الأشياء، وتضمين ضوابط الأمن السيبراني للحوسبة السحابية (CCC) ومراجعتها دوريًا.
٤-٢-٢	وضع سياسات لإدارة التصاريح والصلاحيات والتحقق والتشفير وتقنياتها المناسبة لتأمين أجهزة إنترنت الأشياء التي تتفاعل مع خدمات الحوسبة السحابية المستضافة داخليًا/الخاصة و/أو الخدمات السحابية الأخرى التي تُستخدم خصيصًا لأجهزة إنترنت الأشياء.
٤-٢-٣	تقييم وضع الأمن السيبراني لمقدمي خدمات الحوسبة السحابية و/ أو مقدمي الخدمات المدارة، للتأكد من أن وضع الأمن السيبراني الخاص بهم يتوافق مع سياسات الأمن السيبراني لإنترنت الأشياء وإجراءاته في الجهة.

٤-٢-٤	وضع إجراءات لتسهيل عمليات تدقيق الأمن السيبراني؛ ومراقبة متطلبات الأمن السيبراني لأنشطة معالجة البيانات الخاصة بإنترنت الأشياء، وإدارة المخاطر المحتملة المرتبطة بوجود بيئة متعددة المشتركين في السحابة، وذلك ضمن متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة للجهة.
٤-٢-٥	تضمين أحكاماً في الاتفاقيات التعاقدية مع مقدمي خدمات الحوسبة السحابية و/أو مقدمي الخدمات المُدارة خاصة بالحصول على البيانات المخزنة في المنصات السحابية بصياغة مقروءة لجميع الموردين في حالة خروج مقدم خدمات الحوسبة السحابية و/أو مقدم الخدمات المدارة (بشكل مخطط أو غير مخطط له) من اتفاقية تقديم خدمات الحوسبة السحابية.

ملاحق

ملحق (أ): مبادئ الأمن السيبراني لإنترنت الأشياء للمصنعين

يوضح الجدول (٢) أدناه مبادئ الأمن السيبراني لإنترنت الأشياء، والتي يوصى باتباعها من قبل الشركات المصنعة لتقنية إنترنت الأشياء عند تطوير المنتجات والخدمات.

الرقم	مبادئ الأمن السيبراني لإنترنت الأشياء للمصّنعين
١	**تطبيق** مبادئ "الأمن من خلال التصميم" و " الأمن الإفتراضي" طوال مراحل دورة حياة تطوير أجهزة إنترنت الأشياء وخدماتها.
٢	**إجراء** الإختبارات الأمنية للتأكد من أن الوظائف الأساسية للأمن السيبراني في جهاز إنترنت الأشياء تعمل كما هو متوقع.
٣	**تفعيل** خدمات البرمجيات وبرتوكولات الاتصال المطلوبة لاستخدام وتفعيل الجهاز، فقط.
٤	**تصميم** الأنظمة المضمنة (Embedded Systems) مع وحدة إدارة الذاكرة (MMU) ووحدة حماية الذاكرة (MPU)، لأن المتحكمات الدقيقة وحدها غير قادرة على حماية الذاكرة، ويُنصح مراعاة ذلك عند النشر، وخاصةً عند تشغيل تطبيقات جهات خارجية غير موثوق بها.
٥	**تطبيق** آليات لضمان أن جميع أجهزة إنترنت الأشياء والتطبيقات/البرمجيات المرتبطة بها لا تحتوي على كلمات مرور إفتراضية أو ثابتة.
٦	**تزويد** مستهلكين منتجات إنترنت الأشياء بقائمة تحتوي على مكونات وبرمجيات أجهزة إنترنت الأشياء، بما في ذلك التابعة للأطراف الخارجية.
٧	**إجراء** تقييم مخاطر الأمن السيبراني لسلاسل توريد منتجات إنترنت الأشياء الحساسة.
٨	**ضمان** أن أجهزة إنترنت الأشياء الحساسة لديها القدرة على الفشل بشكل آمن.
٩	**بناء** القدرات الآمنة للتحقق من الهوية في أجهزة إنترنت الأشياء.
١٠	**تقليل** الفرق الزمني ما بين الكشف عن ثغرة في أجهزة إنترنت الأشياء وإصدار التحديثات والإصلاحات اللازمة.
١١	**تبليغ** مستهلكين منتجات إنترنت الأشياء بشكل واضح بوجود تحديثات وإصلاحات أمنية ضرورية مع توضيح المخاطر التي سيعالجها التحديث.

جدول ٢ :مبادئ الأمن السيبراني لإنترنت الأشياء للمصنعين

ملحق (ب): مصطلحات وتعريفات

يوضح الجدول (٣) أدناه بعض المصطلحات وتعريفاتها، التي ورد ذكرها في هذه الإرشادات.

المصطلح	التعريف
القائمة المحددة من التطبيقات Applications Whitelisting	ممارسة أمنية، تتمثل في تحديد قائمة التطبيقات المعتمدة التي يُسمح بتواجدها وتفعيلها على أجهزة المستخدمين والخوادم في الجهة. الهدف من القائمة المحددة هو حماية أجهزة المستخدمين والخوادم من التطبيقات التي قد تكون ضارة.
التحقق Authentication	التأكد من هوية المستخدم أو العملية أو الجهاز، وغالبًا ما يكون هذا الأمر شرطًا أساسيًا للسماح بالوصول إلى الموارد في النظام.
صلاحية المستخدم Authorization	خاصية تحديد والتأكد من حقوق/تراخيص المستخدم للوصول إلى الموارد والأصول المعلوماتية والتقنية للجهة والسماح له وفق ما حدده مسبقا في حقوق/تراخيص المستخدم.
توافر Availability	ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.
التشفير Cryptography	(ويسمى أيضًا علم التشفير) وهي القواعد التي تشتمل مبادئ ووسائل وطرق تخزين ونقل البيانات أو المعلومات في شكل معين وذلك من أجل إخفاء محتواها الدلالي، ومنع الاستخدام غير المصرح به أو منع التعديل غير المكتشف، بحيث لا يمكن لغير الأشخاص المعنيين قراءتها ومعالجتها.
البيانات أثناء التخزين Data-At-Rest	البيانات المخزنة في وسائط التخزين الدائمة؛ مثل الأشرطة (Tapes) والأقراص (Disks).
البيانات أثناء النقل Data-In-Transit	البيانات التي تنتقل من موقع إلى آخر، عن طريق أي نوع من الشبكات؛ مثل الإنترنت، شبكة خاصة... إلخ.
إنترنت الأشياء Internet of Things	الحساسات والأجهزة ("الأشياء") المتصلة بالإنترنت و/أو الشبكات الأخرى، والتي تضيف قيمة، بناءً على البيانات؛ مثل تسهيل المهمات. وتدعم تقنية إنترنت الأشياء العديد من حالات الاستخدام بما في ذلك المنازل الذكية والمدن الذكية والرعاية الصحية الذكية والسيارات الذكية.

المصطلح	التعريف
التحقق من الهوية متعدد العناصر Multi-Factor Authentication (MFA)	نظام أمني يتحقق من هوية المستخدم، ويتطلب استخدام عدة عناصر مستقلة من آليات التحقق من الهوية. تتضمن آليات التحقق عدة عناصر • المعرفة (شيء يعرفه المستخدم فقط (مثل كلمة المرور)). • الحيازة (شيء يملكه المستخدم فقط (مثل برنامج، أو جهاز توليد أرقام عشوائية، أو الرسائل القصيرة المؤقتة لعمليات الدخول ويطلق عليها "One-Time-Password"). • الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط (مثل بصمة الأصبع)).
مبدأ الأمن من خلال التصميم Secure-by-Design	منهجية لتطوير الأنظمة والتطبيقات، وتصميم الشبكات التي تسعى إلى جعلها خالية من نقاط الضعف، والثغرات الأمنية السيبرانية، ولديها المقدرة على صد الهجوم السيبراني قدر الإمكان؛ من خلال عدة تدابير. على سبيل المثال: الاختبار المستمر، وحماية المصادقة والتمسك بأفضل ممارسات البرمجة والتصميم، وغيرها.
مراجعة الشفرة المصدرية Source Code Review	عملية تتم بشكل مؤتمت، أو يدوي؛ لمراجعة الأوامر والتعليمات، المكتوبة بلغة برمجة معينة؛ للبحث عن نقاط الضعف الأمنية فيها.
بيانات القياس عن بُعد Telemetry Data	عملية جمع القياسات والبيانات المتواجدة عن بعد بشكل آلي ونقل تلك البيانات الى نظام مركزي بهدف تحليلها ومراقبتها.

جدول ٣ : مصطلحات وتعريفات

ملحق (ج): قائمة الاختصارات

يوضح الجدول (٤) أدناه، معنى الاختصارات التي ورد ذكرها في هذه الإرشادات.

الاختصار	معناه
CCC	Cloud Cybersecurity Controls ضوابط الأمن السيبراني للحوسبة السحابية
CGIoT	Cybersecurity Guidelines for Inernet of Things إرشادات الأمن السيبراني لإنترنت الأشياء
MMU	Memory Management Unit وحدة إدارة الذاكرة
MPU	Memory Protection Unit وحدة حماية الذاكرة
NCS	National Cryptographic Standards المعايير الوطنية للتشفير
SOC	Security Operations Center مركز عمليات الأمن السيبراني
TLP	Traffic Light Protocol بروتوكول الإشارة الضوئية

جدول ٤: قائمة الاختصارات


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority