الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

# مشروع إرشادات الأمن السيبراني
# لإنترنت الأشياء

Cybersecurity Guidelines for Internet of Things
(CGIoT-1: 2023)

| |
|---|
| إشارة المشاركة: أبيض |
| تصنيف الوثيقة: عام |

بسم الله الرحمن الرحيم

تنويه: 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 إلزامية؛ فإن المتطلبات الإلزامية 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 تشريعاتها -بإجراء تقييمات دورية لتلك المخاطر.

# بروتوكول الإشارة الضوئية (TLP):

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

- **أحمر – شخصي وسري للمستلم فحسب**

  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

# 1. الملخص التنفيذي

تبنت المملكة العربية السعودية (رؤية 2030) لتكون خارطة طريق؛ لتحقيق النمو الاقتصادي والتنمية الوطنية. وحددت الرؤية الأهداف العامة للمملكة والمستهدفات اللازمة لتمكينها من أن تكون نموذجًا عالميًا لدولة ناجحة ورائدة. وتعتزم المملكة العربية السعودية بناء مجتمع رقمي مزدهر؛ يُعد التبني الواسع النطاق لإنترنت الأشياء عامل تمكين رئيسي فيه.

ومن هذا المنطلق؛ قامت الهيئة الوطنية للأمن السيبراني بإعداد إرشادات الأمن السيبراني لإنترنت الأشياء (CGIoT-1:2023) من خلال تحديد المبادئ التوجيهية 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.

يعنى مكون (حوكمة الأمن السيبراني) بضمان كون الإستراتيجية، والرؤية، وخارطة الطريق، والأهداف للجهة؛ تضع في الحسبان الأمن السيبراني لإنترنت الأشياء. ويشمل ذلك الالتزام بالتنظيمات والتشريعات ذات العلاقة. ويُعنى هذا المحور 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، وإدراج 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. وفيما يخص مكون (تعزيز الأمن السيبراني)، فإنه يعنى بضمان تطبيق آليات الأمن السيبراني الملائمة لتقنية إنترنت الأشياء من أجل حماية المعلومات وأصولها ضد الهجمات السيبرانية. في حين يعنى مكون (صمود الأمن السيبراني) بتعزيز قدرة الجهة على الصمود أمام الآثار المترتبة على الكوارث التي قد تطرأ بسبب الحوادث المتعلقة بالأمن السيبراني لإنترنت الأشياء. ويعنى 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.

# 2. المقدمة

يشير مصطلح إنترنت الأشياء الى الحساسات و الأجهزة ("الأشياء") المتصلة بالإنترنت و/أو الشبكات الأخرى والتي تضيف قيمة بناءً على البيانات؛ مثل تسهيل المهام. وتدعم تقنية إنترنت الأشياء العديد من حالات الاستخدام بما في ذلك المنازل الذكية والمدن الذكية والرعاية الصحية الذكية والسيارات الذكية. وتؤدي تقنية إنترنت الأشياء دوراً هاماً في تحسين مستويات المعيشة، وتحقيق التحول الرقمي الذكي، والتنمية المجتمعية المستدامة، ونظراً للتبني الواسع لهذة التقنية، قد تكون الجهات المستخدمة لتقنية إنترنت الأشياء أكثر عرضة للتهديدات والمخاطر السيبرانية.

وعليه؛ قامت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") بإعداد إرشادات الأمن السيبراني لإنترنت الأشياء (CGIoT-1: 2023) وذلك بعد إجراء دراسة شاملة لعدة إرشادات ومعايير وأطر وضوابط عالمية تتعلق بالأمن السيبراني، وتحليل الوضع الراهن والمتطلبات التشريعية والتنظيمية في مجال تقنية إنترنت الأشياء في المملكة، وتحليل ماتم رصده من الحوادث والهجمات السيبرانية السابقة المتعلقة بإنترنت الأشياء.

تتكون إرشادات الأمن السيبراني لإنترنت الأشياء مما يلي:

- 4 مكونات أساسية (Main Domains)
- 27 مكونًا فرعيًا (Subdomains)
- 80 إرشادًا (Guidelines)

# 3. الأهداف

تهدف هذه الإرشادات إلى تضمين أفضل ممارسات الأمن السيبراني لدى الجهات التي تستخدم تقنية إنترنت الأشياء. وتستند هذه الممارسات إلى المعايير الرائدة مما يساعد الجهات على تقليل 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، يجب تضمين 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)

# 4. نطاق العمل وقابلية التطبيق

توصي الهيئة الجهات التي تستخدم إنترنت الأشياء، والشركات المصنّعة لها، ومقدمو الخدمات لمنتجاتها في المملكة (ويشار لها جميعًا في هذه الوثيقة باسم "الجهة") على اتباع الإرشادات؛ بهدف ضمان تطبيق أفضل الممارسات، والتقليل من مخاطر الأمن السيبراني، التي قد تنتج من استخدام هذه التقنية.

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

# 5. مكونات وهيكلية إرشادات الأمن السيبراني لإنترنت الأشياء

## 5.1 المكونات الأساسية والفرعية، لإرشادات الأمن السيبراني لإنترنت الأشياء

يوضح الشكل (1) أدناه، المكونات الأساسية والفرعية، لإرشادات الأمن السيبراني لإنترنت الأشياء

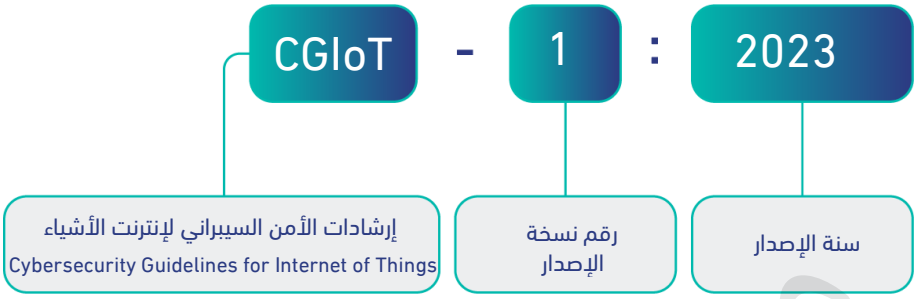
| | | | | |
|---|---|---|---|---|
| 1 - حوكمة الأمن السيبرانى Cybersecurity Governance | 1-1 | استراتيجية الأمن السيبراني Cybersecurity Strategy | 2-1 | سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures |
| | 3-1 | أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities | 4-1 | إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management |
| | 5-1 | الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information and Technology Project Management | 6-1 | الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Compliance with Cybersecurity Standards, Laws and Regulations |
| | 7-1 | المراجعة والتدقيق الدوري للأمن السيبراني Periodical Cybersecurity Review and Audit | 8-1 | الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources |
| | 9-1 | برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program | | |
| 2 - تعزيز الأمن السيبرانى Cybersecurity Defense | 1-2 | إدارة الأصول Asset Management | 2-2 | إدارة هويات الدخول والصلاحيات Identity and Access Management |
| | 3-2 | حماية البريد الإلكتروني وأنظمة الرسائل الإلكترونية Email and Messaging Services Protection | 4-2 | إدارة أمن الشبكات Network Security Management |
| | 5-2 | أمن الأجهزة المحمولة المتصلة بإنترنت الأشياء IoT-Connected Mobile Device Security | 6-2 | حماية البيانات والمعلومات Data and Information Protection |
| | 7-2 | التشفير Cryptography | 8-2 | إدارة النسخ الاحتياطية Backup and Recovery Management |

| | | | | |
|---|---|---|---|---|
| | 9-2 | إدارة الثغرات<br>Vulnerability Management | 10-2 | اختبار الاختراق<br>Penetration Testing |
| | 11-2 | إدارة سجلات الأحداث ومراقبة الأمن السيبراني<br>Cybersecurity Event Logs and Monitoring Management | 12-2 | إدارة حوادث وتهديدات الأمن السيبراني<br>Cybersecurity Incident and Threat Management |
| | 13-2 | الأمن المادي<br>Physical Security | 14-2 | أمن تطبيقات إنترنت الأشياء<br>IoT Application Security |
| | 15-2 | إدارة دورة حياة أجهزة إنترنت الأشياء<br>IoT Device Lifecycle Management | | |
| 3. صمود الأمن السيبراني Cybersecurity Resilience | 1-3 | جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال<br>Cybersecurity Resilience Aspects of Business Continuity Management (BCM) | | |
| 4. الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third Party and Cloud Computing Cybersecurity | 1-4 | الأمن السيبراني المتعلق بالأطراف الخارجية<br>Third-Party Cybersecurity | 2-4 | الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة<br>Cloud Computing and Hosting Cybersecurity |

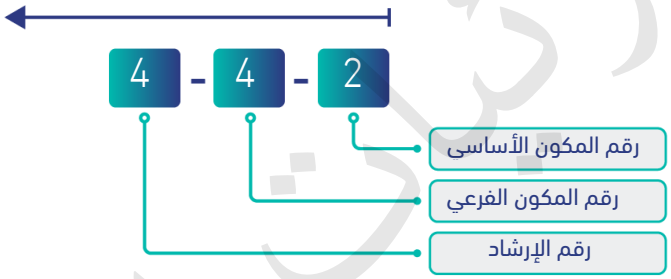
شكل 1:المكونات الأساسية والفرعية لإرشادات الأمن السيبراني لإنترنت الأشياء

## 5.2 الهيكلية

يوضح الشكلان (2) و (3) أدناه معنى رموز إرشادات الأمن السيبراني لإنترنت الأشياء




شكل 2 : معنى رموز إرشادات الأمن السيبراني لإنترنت الأشياء




شكل 3 : هيكلية إرشادات الأمن السيبراني لإنترنت الأشياء

يوضح الجدول (1) أدناه طريقة هيكلية إرشادات الأمن السيبراني لإنترنت الأشياء.

| | |
|---|---|
| 1<br>رقم مرجعي للمكون الأساسي | اسم المكون الأساسي |
| رقم مرجعي للمكون الفرعي | اسم المكون الفرعي |
| الهدف | |
| الإرشادات | |
| رقم مرجعي للإرشاد | بنود الإرشاد |

جدول 1 : هيكلية إرشادات الأمن السيبراني لإنترنت الأشياء

# 6. إرشادات الأمن السيبراني لإنترنت الأشياء

## 1 حوكمة الأمن السيبراني (Cybersecurity Governance)

| | |
|---|---|
| 1-1 | استراتيجية الأمن السيبراني |
| الهدف | ضمان احتواء الإستراتيجيات ورؤى وخطط العمل والأهداف والمبادرات والمشاريع للأمن السيبراني في الجهة، على جوانب الأمن السيبراني الخاصة بإنترنت الأشياء، وإسهامها في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة. |
| الإرشادات | |
| 1-1-1 | تحديد متطلبات الأمن السيبراني لإنترنت الأشياء ضمن استراتيجية الأمن السيبراني الخاصة بالجهة وتوثيقها واعتمادها. |
| 2-1-1 | 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. |
| 3-1-1 | تحديد مؤشرات الأداء الرئيسية للأمن السيبراني لإنترنت الأشياء، ومتابعتها؛ لضمان تلبية متطلبات الأمن السيبراني طوال دورة حياة أجهزة إنترنت الأشياء. |
| 4-1-1 | 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. |
| 2-1 | سياسات وإجراءات الأمن السيبراني |
| الهدف | ضمان التوثيق والنشر لسياسات الأمن السيبراني لإنترنت الأشياء واجراءته، والتزام الأطراف المعنيين داخل الجهة بها، وكذلك الأطراف الخارجية ذات العلاقة، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة. |
| الإرشادات | |
| 1-2-1 | 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 خدمات الإسناد ومقدمي الخدمات من الأطراف الخارجية. |
| 2-2-1 | الحرص على دعم السياسات والإجراءات بمعايير تقنية أمنية على سبيل المثال (التحصينات / الحد الأدنى من معايير الأمان الأساسية للأنظمة المضمنة، ومعايير التحقق والصلاحيات للمستخدم، والشهادات الرقمية، ومعايير أمن تقسيم الشبكة، وما إلى ذلك). |
| 3-2-1 | 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. |

| | |
|---|---|
| 3-1 | أدوار ومسؤوليات الأمن السيبراني |
| الهدف | ضمان تحديد الأدوار والمسؤوليات لجميع الأطراف المعنية بالإدارة والتنفيذ والمراقبة لمتطلبات الأمن السيبراني لإنترنت الأشياء داخل الجهة. |
| الإرشادات | |
| 1-3-1 | 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. |
| 2-3-1 | 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. |
| 4-1 | 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 | |
| 1-4-1 | 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. |
| 2-4-1 | تحديد قائمة بسيناريوهات المخاطر الشائعة التي يمكن أن تؤثر على أجهزة إنترنت الأشياء أو المنظومة المرتبطة بها أو الجهة. |
| 3-4-1 | تحديد مخاطر الأمن السيبراني لإنترنت الأشياء وتوثيقها في سجل مخاطر الأمن السيبراني لإنترنت الأشياء ضمن السجل العام لمخاطر الأمن السيبراني للجهة. |
| 4-4-1 | إجراء تقييم مخاطر الأمن السيبراني لإنترنت الأشياء مع الأخذ في الاعتبار التهديدات المحتملة لإنترنت الأشياء والسيناريوهات المحتملة لهجمات إنترنت الأشياء الشائعة واحتمالية تعطيل العمليات والأضرار المرتبطة بها. |
| 5-4-1 | تحديد مخاطر الأمن السيبراني التي تتجاوز مستوى المخاطر المقبول وتحديد التدابير المناسبة لمعالجة هذه المخاطر وتقليل مستوى هذه المخاطر إلى المستوى المقبول في الجهة أو أقل منه. |
| 6-4-1 | 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. |

| | |
|---|---|
| 5-1 | الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية |
| الهدف | ضمان تضمين 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 | |
| 1-5-1 | تطبيق الممارسات الوطنية والدولية الرائدة المتعلقة بمبادئ "التصميم الآمن" طوال مراحل دورة حياة تطوير أجهزة/خدمات إنترنت الأشياء. |
| 2-5-1 | مراجعة أجهزة/خدمات إنترنت الأشياء؛ لضمان مراعاتها لمتطلبات الأمن السيبراني، أثناء مراحل التخطيط والتصميم، للمشاريع المعلوماتية والتقنية. |
| 3-5-1 | تحديد إجراءات إدارة التغيير لإنترنت الأشياء لضمان التحكم في حالة الأمن السيبراني لإنترنت الأشياء في الجهة. ومنها:<br>■ مراعاة أنشطة إدارة التغيير عبر مراحل دورة حياة أجهزة إنترنت الأشياء، بما في ذلك مرحلة التطوير والتكامل، ومرحلة الصيانة أو التخلص، وكذلك أثناء التحديثات أو التصحيحات أو تغييرات الوظائف.<br>■ مراقبة التغيير ونشره إلى الأطراف ذات العلاقة داخل الجهة. |
| 6-1 | 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 | |
| 1-6-1 | تطبيق آليات إنفاذ والتزام مناسبة لضمان توافق المتطلبات والبرامج والمبادرات والأنشطة التنظيمية، المتعلقة بإنترنت الأشياء، مع المتطلبات التشريعية والتنظيمية والمعايير المتعلقة بالأمن السيبراني. |
| 7-1 | 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، والاتفاقيات الدولية المقرة تنظيميًا على الجهة. |
| الإرشادات | |
| 1-7-1 | مراجعة تطبيق متطلبات الأمن السيبراني لإنترنت الأشياء، داخل الجهة، بشكل دوري، من قبل إدارة الأمن السيبراني. |
| 2-7-1 | 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. |
| 3-7-1 | 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. |

| | |
|---|---|
| 8-1 | 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 | |
| 1-8-1 | تحديد متطلبات الأمن السيبراني لإنترنت الأشياء للعاملين في الجهة قبل التوظيف وأثناء توظيف العاملين، وبعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة وتوثيقها واعتمادها. ويشمل ذلك ما يلي:<br>■ التعريف بمتطلبات الأمن السيبراني، وتوثيق متطلبات التدريب المستمر للعاملين، مع العناية بشكل خاص بمتطلبات الأمن السيبراني لإنترنت الأشياء.<br>■ تنفيذ متطلبات الأمن السيبراني لإنترنت الأشياء، والامتثال لها. |
| 2-8-1 | مراجعة صلاحيات وصول العاملين إلى أصول إنترنت الأشياء بشكل دوري، وتحديثها، أو إلغاؤها فوراً عند تغيير أدوار العاملين، أو إنهاء/انتهاء العلاقة الوظيفية، وفقًا لمبادئ الحاجة إلى المعرفة، والاستخدام، والحد الأدنى من الصلاحيات والامتيازات. |
| 3-8-1 | 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. |
| 9-1 | 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 | |
| 1-9-1 | تضمين جوانب الأمن السيبراني لإنترنت الأشياء، ضمن برنامج التوعية بالأمن السيبراني واستراتيجية التدريب داخل الجهة. ويشمل ذلك على ما يلي:<br>■ تحديد استراتيجية تدريب العاملين ذوي المهامات الوظيفية المتعلقة بإنترنت الأشياء؛ وتوثيقها واعتمادها.<br>■ تدريب العاملين على أفضل ممارسات الأمن السيبراني من أجل ضمان الاستخدام الآمن لأجهزة إنترنت الأشياء وخدماتها.<br>■ تضمين البرامج التدريبية بأفضل الممارسات المطبقة، ومهمات الأمن السيبراني لإنترنت الأشياء ومسؤولياته، والسياسات والمعايير؛ لضمان بيئة عمل آمنة. |

| | |
|---|---|
| 2-9-1 | تعزيز الوعي بالأمن السيبراني لإنترنت الأشياء، على جميع مستويات الجهة؛ مع مراعاة الآتية:<br>■ توعية العاملين في جميع مستويات الجهة بأهمية حماية أجهزة إنترنت الأشياء؛ بما في ذلك صناع القرار.<br>■ تنفيذ أنشطة التوعية بالأمن السيبراني؛ لزيادة الوعي بالأمن السيبراني لإنترنت الأشياء بين العاملين؛ من خلال الدورات التدريبية والمحاكاة، والمحادثات، وتعميم كتيبات أفضل ممارسات الأمن السيبراني ذات العلاقة بإنترنت الأشياء، عبر البريد الإلكتروني، وخلال الاجتماعات وغيرها من طرق التوعية وقنواتها.<br>■ تقييم مهارات الأمن السيبراني في إنترنت الأشياء للعاملين عليها؛ من أجل تحديد الفجوات المعرفية، وتخطيط التدريب، بناء على المهارات المطلوبة لكل وظيفة.<br>■ إبقاء العاملين الذين يستخدمون أجهزة إنترنت الأشياء، على اطلاع مستمر، بأحدث التطورات في هذا المجال. |

## ٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

| | |
|---|---|
| 1-2 | إدارة الأصول |
| الهدف | ضمان امتلاك الجهة، لقائمة جرد دقيقة، ومفصلة، وحديثة لجميع الأصول ذات العلاقة بإنترنت الأشياء من أجل الحفاظ على سريتها، وسلامتها، وتوافرها، بما يتسق مع متطلبات الأمن السيبراني، ودعم العمليات التشغيلية في الجهة. |
| الإرشادات | |
| 1-1-2 | إنشاء قائمة جرد للأنواع المختلفة من أجهزة إنترنت الأشياء التي تستخدمها الجهة، بحيث تشتمل على التصنيف، 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. |
| 2-1-2 | إجراء المراجعات الدورية لقائمة جرد أصول إنترنت الأشياء ومتابعة جميع التغييرات داخل الجهة. |
| 2-2 | 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 | |
| 1-2-2 | إدارة هويات الدخول وصلاحياتها، إلى أصول إنترنت الأشياء، وتقييد الوصول إلى بياناتها وأجهزتها على المستخدمين المصرح لهم فحسب، بناءً على مبادئ التحكم بالدخول والصلاحيات (مبدأ الحاجة إلى المعرفة والاستخدام، ومبدأ الحد الأدنى من الصلاحيات والامتيازات، ومبدأ فصل المهمات). |
| 2-2-2 | تطبيق معايير عالية، للتحقق من الهوية، واتباع أفضل الممارسات وهي:<br>■ إلزام المستخدمين، بعدم استخدام كلمات المرور، الثابتة والافتراضية.<br>■ زيادة تعقيد كلمات المرور الفريدة؛ مثل تحديد الحد الأدنى لطول الكلمة، واستخدام مجموعة من الأحرف (الأحرف الكبيرة والصغيرة) والأرقام والرموز.<br>■ منع عرض كلمة مرور المستخدم على واجهات تسجيل الدخول في التطبيقات.<br>■ وضع حد أقصى لمحاولات الدخول الخاطئة.<br>■ تفعيل التحقق من الهوية متعدد العناصر. |
| 3-2-2 | إجراء المراجعات لهويات الدخول والصلاحيات؛ بناءً على مبادئ التحكم بالدخول والصلاحيات. |
| 3-2 | 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 | |

| | |
|---|---|
| 1-3-2 | تحديد متطلبات الأمن السيبراني لحماية البيانات المنقولة بين أجهزة إنترنت الأشياء وخدمات البريد الإلكتروني والرسائل بالجهة وتوثيقها واعتمادها ومراجعتها دورياً. |
| 2-3-2 | تطبيق متطلبات الأمن السيبراني لحماية البيانات المنقولة بين أجهزة إنترنت الأشياء وخدمات البريد الإلكتروني والرسائل بالجهة، ضمن إجراءات حماية خدمات البريد الإلكتروني والرسائل للجهة. |
| 4-2 | إدارة أمن الشبكات |
| الهدف | تطوير قدرات اتصال، وتكامل آمنة وموثوقة، بين أجهزة إنترنت الأشياء المختلفة في الشبكة. |
| الإرشادات | |
| 1-4-2 | تحديد متطلبات الأمن السيبراني للاتصال الآمن بين أجهزة إنترنت الأشياء، وبيئة الاستخدام بما في ذلك الأجهزة الأخرى والبنية التحتية التقنية/السحابية وتوثيقها، واعتمادها، ومراجعتها دورياً. |
| 2-4-2 | تطبيق تدابير لتأمين اتصال البيانات، ونقلها بين الأجهزة المختلفة المتصلة في الشبكة، بما في ذلك مصادقة أجهزة إنترنت الأشياء الأخرى (الأجهزة النظيرة "Peer Devices") التي تحاول الإتصال بها. |
| 3-4-2 | تشفير عمليات انتقال البيانات بين أجهزة إنترنت الأشياء، والمصادقة عليها؛ بالإضافة إلى تأمين البنية التحتية الأساسية. |
| 4-4-2 | تطبيق العزل والتقسيم المنطقي و/ أو المادي بين بيئة إنترنت الأشياء، وبيئة الجهة، بناءً على دراسة المخاطر السيبرانية لدى الجهة. |
| 5-4-2 | استخدام خوادم التحديث الآمنة، لضمان النقل الآمن لملفات التحديث الخاصة ببرمجيات/البرامج الثابتة لأجهزة إنترنت الأشياء، وإعداداتها، وتطبيقاتها ووضع آليات مصادقة وتشفير مناسبة، لنقل التحديثات. |
| 5-2 | أمن الأجهزة المحمولة المتصلة بإنترنت الأشياء |
| الهدف | ضمان تطبيق متطلبات الأمن السيبراني، للأجهزة المحمولة، المتصلة بإنترنت الأشياء؛ لتعزيز حمايتها، وتقليل مخاطر الأمن السيبراني فيها. |
| الإرشادات | |
| 1-5-2 | تطبيق التدابير الآتية للأجهزة المحمولة المتصلة بإنترنت الأشياء:<br>■ تنفيذ تدابير، لتأمين الاتصال بين جهاز إنترنت الأشياء، والأجهزة المحمولة.<br>■ تقييد الوصول إلى الأجهزة المحمولة، المتصلة بإنترنت الأشياء، على المستخدمين المصرح لهم فحسب.<br>■ استخدام طرق المصادقة الآمنة، للوصول إلى بيانات الجهاز المحمول، وجهاز إنترنت الأشياء.<br>■ تنفيذ الممارسات الآمنة، عند تطوير البرمجيات، لتطبيقات الأجهزة المحمولة، التي تتفاعل مع أجهزة إنترنت الأشياء.<br>■ الحذف الآمن لبيانات أجهزة إنترنت الأشياء، المخزنة على الأجهزة المحمولة؛ عند فقدان تلك الأجهزة المحمولة، أو عند انتهاء الحاجة إلى استخدامها. |
| 6-2 | حماية البيانات والمعلومات |
| الهدف | ضمان سرية البيانات التي تتم معالجتها بواسطة أجهزة إنترنت الأشياء وكذلك ضمان سلامتها وتوافرها. |
| الإرشادات | |

| | |
|---|---|
| 1-6-2 | تطبيق آليات لتصنيف البيانات الخاصة بأجهزة إنترنت الأشياء وترميزها؛ حسب التشريعات والتنظيمات ذات العلاقة، والمتطلبات التنظيمية في الجهة. |
| 2-6-2 | تطبيق تدابير الحماية؛ لتجنب الوصول إلى البيانات المتعلقة بإنترنت الأشياء، أو العبث بها عند تخزينها، أو أثناء نقلها. |
| 3-6-2 | منع أجهزة إنترنت الأشياء من جمع البيانات الحساسة غير المطلوبة أو التي لا يمكن حمايتها بشكلٍ كافٍ. |
| 7-2 | التشفير |
| الهدف | ضمان الاستخدام المناسب للتشفير بهدف تأمين معاملات البيانات وتبادلها بين أجهزة إنترنت الأشياء. |
| الإرشادات | |
| 1-7-2 | تحديد متطلبات الأمن السيبراني لإنترنت الأشياء فيما يخص تشفير بيانات إنترنت الأشياء، وفقًا للمعايير الوطنية للتشفير (NCS-1:2020) وتوثيقها، واعتمادها، ومراجعتها دوريًا. |
| 2-7-2 | تشفير البيانات، سواء أكان ذلك أثناء التخزين، أم أثناء النقل. |
| 8-2 | إدارة النسخ الاحتياطية |
| الهدف | ضمان النسخ الاحتياطي، واستعادة البيانات داخل أجهزة إنترنت الأشياء؛ وذلك بهدف حماية البيانات التي تتم معالجتها بواسطة هذه الأجهزة من الأضرار الناجمة عن المخاطر السيبرانية. |
| الإرشادات | |
| 1-8-2 | تحديد متطلبات الأمن السيبراني لإنترنت الأشياء لإدارة النسخ الاحتياطية واستعادة عمل الأنظمة والبيانات، ضمن سياسات إدارة النسخ الاحتياطية والاستعادة، في الجهة وتوثيقها، واعتمادها، ومراجعتها دوريًا. |
| 2-8-2 | توفير نسخة مجربة وموثوقة، من بيانات وبرمجيات إنترنت الأشياء للتمكن؛ من استعادة البيانات بشكل آمن. |
| 3-8-2 | إجراء المراجعات الدورية للنسخ الاحتياطية المخزنة لأجهزة إنترنت الأشياء واختبارها. |
| 9-2 | إدارة الثغرات |
| الهدف | ضمان اكتشاف الثغرات الأمنية في الوقت المناسب، ومعالجتها بشكل فعال، وذلك لمنع احتمالية استغلالها في شن الهجمات السيبرانية وتقليل الآثار المترتبة على أعمال الجهة. |
| الإرشادات | |
| 1-9-2 | فحص واكتشاف ثغرات الأمن السيبراني ومراقبتها باستمرار ومعالجتها في أجهزة إنترنت الأشياء. |
| 2-9-2 | تنصيب التحديثات والإصلاحات على جميع مكونات البرمجيات، ضمن أجهزة إنترنت الأشياء في الوقت المناسب حسب الآتي:<br>■ تنفيذ تصحيحات البرمجيات بطريقة وقائية، مثل التحديثات التلقائية؛ لضمان الحد من ثغرات الأمن السيبراني، قبل أن يتم استغلالها.<br>■ المحافظة على الأداء الأساسي للأجهزة، أثناء تنصيب التحديثات والإصلاحات.<br>■ استخدام أحدث نظم التشغيل، عند تطوير أجهزة إنترنت الأشياء، بحيث يساعد في ضمان التقليل من الثغرات المعروفة. |

| 10-2 | اختبار الاختراق |
|---|---|
| الهدف | تقييم كفاءة الأمن السيبراني لإنترنت الأشياء وتعزيز قدراته داخل الجهة؛ من خلال عمل محاكاة الهجمات السيبرانية لتحديد نقاط الضعف غير المعروفة، التي قد تؤدي إلى اختراقات سيبرانية. |
| الإرشادات | |
| 1-10-2 | تنفيذ عمليات اختبار الاختراق؛ من أجل اكتشاف الثغرات، التي قد تواجه برامج إنترنت الأشياء، ومكونات الأجهزة استباقيًا وذلك عن طريق:<br>■ تحديد أصول إنترنت الأشياء ضمن نطاق عمل اختبار الاختراق وتحليلها.<br>■ التحقق من الثغرات المعروفة واختبار قابلية استغلالها؛ إلى جانب التعرف على أي ثغرات أمنية لم تكن معروفة مسبقًا (Zero-Day Vulnerabilities) في أجهزة إنترنت الأشياء.<br>■ تحديد الإعدادات غير الآمنة وتقييمها على مستوى التطبيق، والشبكة والبيانات و/أو على مستوى الحساسات، أو بوابة الجهاز.<br>■ تطبيق الإجراءات المناسبة، للإبلاغ والتحذير؛ من أجل المساعدة في ترتيب أولويات اتخاذ القرارات المتعلقة بمكان تضمين تدابير الأمن السيبراني الإضافية وكيفية ذلك. |
| 2-10-2 | تنفيذ تمارين فريق اختبار الكفاءات الدفاعية؛ وذلك باستهداف أجهزة إنترنت الأشياء وخدماتها ذات المهمات الحساسة، لمحاكاة الهندسة الاجتماعية، والوصول المادي، والاختراق، وغيرها من التقنيات الخادعة، التي تهدف إلى الوصول غير المصرح إلى المعلومات، والأصول الحساسة. |
| 11-2 | إدارة سجلات الأحداث ومراقبة الأمن السيبراني |
| الهدف | ضمان جمع سجلات أحداث الأمن السيبراني لإنترنت الأشياء ومراقبتها وتحليلها، وحالات التهديد، على نحو منتظم، وذلك بهدف تمكين الكشف المبكر عن أي هجمات إلكترونية محتملة عبر مكونات أجهزة إنترنت الأشياء وخدماتها التي يمكن أن تكون مرتبطة بحوادث الأمن السيبراني. |
| الإرشادات | |
| 1-11-2 | تمكين أجهزة إنترنت الأشياء من تسجيل أحداث الأمن السيبراني، ورصد البيانات وتخزينها مركزيًا ونقلها إلى مركز عمليات مراقبة الأمن السيبراني (SOC) في الجهة مع مراعاة الآتي:<br>■ تحديد السيناريوهات لاكتشاف حوادث الأمن السيبراني المحتملة لإنترنت الأشياء.<br>■ تسجيل الأحداث مثل التحقق من هوية المستخدمين، وإدارة الحسابات، وصلاحيات الوصول ومحاولات الوصول إلى البيانات الحساسة، والتعديلات على موارد النظام.<br>■ مراقبة سجلات الأحداث والتهديدات ومراجعتها وتحليلها على نحو منتظم، وتنفيذ أنظمة آلية؛ لتمكين المراقبة المباشرة للسجلات والتهديدات؛ إن أمكن.<br>■ 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 لتمكين الاستعادة الآمنة لبيانات السجلات. |

| | |
|---|---|
| | ▪ عند رصد تغيير أو سلوك غير مصرح به في برمجية 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.<br>▪ تحليل سوء الاستخدام المحتمل لصلاحيات الوصول من قبل الأطراف المعنية داخليًا.<br>▪ فحص بيانات القياس عن بُعد (Telemetry Data) التي تم جمعها بواسطة أجهزة إنترنت الأشياء وخدماتها؛ مثل بيانات الاستخدام، والقياس، والسجلات، لاكتشاف الحالات المشبوهة في الأمن السيبراني، وتحديد الظروف غير العادية في الوقت المناسب.<br>▪ تحديد فترة الاحتفاظ ببيانات أحداث الأمن السيبراني؛ بحيث تكون لاتقل عن 12 شهرًا على الأقل من تاريخ تسجيلها. |
| 2-11-2 | فحص المعلومات التشخيصية بانتظام؛ 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. |
| 12-2 | 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 | |
| 1-12-2 | تضمين نموذج إدارة الحوادث، والتهديدات الخاصة بإنترنت الأشياء، ضمن أنشطة إدارة حوادث وتهديدات الأمن السيبراني وبرامجها للجهة. |
| 2-12-2 | وضع خطة لإدارة حوادث الأمن السيبراني لإنترنت الأشياء؛ لتشمل الاستجابة للحوادث، وإجراءات المعالجة بما يتسق مع ممارسات إدارة الحوادث للجهة؛ ومنها:<br>▪ الاستعداد للحوادث؛ من خلال التأكد من كون الأنظمة والشبكات والتطبيقات آمنة.<br>▪ كشف الحوادث وتحليلها وتوثيقها.<br>▪ إبلاغ الأطراف المعنية عن الحوادث ومنها الهيئة الوطنية للأمن السيبراني.<br>▪ احتواء الحوادث، ومعالجتها، والتعافي من آثارها.<br>▪ إعداد تقارير متابعة عن الحوادث. |
| 3-12-2 | تطوير قدرات إجراء التحليلات اللازمة، بعد كل حادث؛ للكشف عن عناصر البرمجيات والأجهزة والمكونات لجهاز 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 أو القديمة، التي تحتوي على كلمات مرور افتراضية. |
| 4-12-2 | 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:<br>▪ تتبع المعلومات الاستباقية المستخلصة من استخدام أجهزة أو خدمات إنترنت الأشياء ومراقبتها وتوثيقها.<br>▪ مشاركة المعلومات المتعلقة بمؤشرات الاختراقات؛ والمعلومات الاستباقية مع الهيئة الوطنية للأمن السيبراني. |

| | |
|---|---|
| | ▪ مراجعة متطلبات الأمن السيبراني لإنترنت الأشياء لإدارة التهديدات دورياً. |
| 13-2 | الأمن المادي |
| الهدف | ضمان حماية أصول إنترنت الأشياء، من الوصول المادي غير المصرح به؛ وكذلك الحماية من الفقد والسرقة والتلف. |
| الإرشادات | |
| 1-13-2 | 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. |
| 2-13-2 | تنفيذ التدابير اللازمة؛ لحماية أجهزة إنترنت الأشياء، من محاولات العبث المادي، بها ورصد تلك المحاولات. |
| 14-2 | أمن تطبيقات إنترنت الأشياء |
| الهدف | ضمان أمان تطبيقات البرامج التي تعمل على أجهزة إنترنت الأشياء وكذلك ضمان موثوقيتها. |
| الإرشادات | |
| 1-14-2 | تنفيذ تدابير الأمن السيبراني التقنية؛ لتأمين واجهات تطبيقات إنترنت الأشياء، للحد من الكشف عن البيانات، والإعدادات، وعمليات الإدارة، ومنع الوصول غير المصرح به. |
| 2-14-2 | 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. |
| 3-14-2 | تنفيذ ممارسات التطوير البرمجية الآمنة؛ لتطبيقات إنترنت الأشياء، ومراجعة الشفرة، لتلافي الأخطاء البرمجية ذات التأثير على الأمن السيبراني أو الحد منها. |
| 4-14-2 | تحديث قائمة التطبيقات المسموح بها، بشكل دوري؛ لتشمل التطبيقات والخصائص، والتحديثات والإصلاحات البرمجية. |
| 15-2 | إدارة دورة حياة أجهزة إنترنت الأشياء |
| الهدف | ضمان التثبيت والإعداد الآمن لأجهزة إنترنت الأشياء؛ بالإضافة إلى التحديث، والتصحيح للنظام بشكل منتظم، وإيجاد خطط سحب واستبدال للأجهزة. |
| الإرشادات | |
| 1-15-2 | استخدام الأجهزة التي تتضمن وظائف الأمن السيبراني على مستوى المكونات؛ للحفاظ على حماية الأجهزة وسلامتها، مع اتباع الآتي:<br>▪ 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.<br>▪ حصر استخدام منافذ أجهزة إنترنت الأشياء الخارجية، على المنافذ الضرورية فحسب، لعمل الجهاز وضمان موثوقية الأجهزة المتصلة بها. |

| | |
|---|---|
| | ▪ 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. |
| 2-15-2 | تحديد خطوات تثبيت أجهزة إنترنت الأشياء وخدماتها، وإعدادها. ويُنصح أن تتوافق هذه الخطوات مع أفضل ممارسات الأمن السيبراني، فيما يتعلق بإمكانية استخدام الأجهزة أو الخدمات، ومنها:<br>▪ تطبيق الإعدادات الآمنة وخيارات التحصينات التي تنطبق على الجهة، مثل تعطيل سمات، أو وظائف معينة، لن تستخدمها الجهة.<br>▪ تجهيز أجهزة إنترنت الأشياء واعدادها بطريقة آمنة، مثل ضمان كون جميع الأجهزة والتطبيقات/الخدمات المرتبطة بها؛ لا تحتوي على كلمة مرور افتراضية، وأن تكون كلمات المرور فريدة ومعقدة.<br>▪ تنفيذ اختبارات الأمن السيبراني؛ قبل نشر التطبيق في بيئة الإنتاج.<br>▪ إجراء اختبارات الأمن السيبراني بشكل دوري؛ قبل كل إصدار جديد للبرمجيات وبعده. |
| 3-15-2 | وضع خطة معنية بسحب أجهزة إنترنت الأشياء أو خدماتها في نهاية دورة حياتها. بالإضافة إلى تنفيذ الممارسات الآتية لوضع استراتيجية عند نهاية العمر الافتراضي لأجهزة إنترنت الأشياء وخدماتها:<br>▪ وضع خطة استبدال، وخطة نهاية العمر الافتراضي لأجهزة إنترنت الأشياء، التي انتهى الضمان الخاص بها ولم تعد تدعم متطلبات الأمن السيبراني الأساسية. بالإضافة إلى تضمين مكونات الجهات الخارجية في خطة نهاية العمر الافتراضي للأجهزة والخدمات.<br>▪ تنفيذ تدابير لإتلاف البيانات التي تم تخزينها، أو معالجتها، بواسطة جهاز/خدمة إنترنت الأشياء، وفقًا للسياسات واللوائح التنظيمية ذات العلاقة في الجهة.<br>▪ الاحتفاظ بسجل تدقيق لمراقبة عملية التخلص من أجهزة إنترنت الأشياء وخدماتها. |

## 3 صمود الأمن السيبراني( Cybersecurity Resilience )

| 1-3 | 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 أثناء حوادث الأمن السيبراني. |
| الإرشادات | |
| 1-1-3 | تضمين متطلبات صمود الأمن السيبراني في الحفاظ، على سرية أجهزة إنترنت الأشياء والمكونات المرتبطة بها وسلامتها وتوافرها؛ ضمن خطة إدارة استمرارية الأعمال للجهة. وتنفيذ الممارسات الآتية:<br>■ تطوير متطلبات الصمود، مع مراعاة ماهية تأثير تعطيل الوظائف الأساسية لأجهزة إنترنت الأشياء بسبب الهجمات السيبرانية على إجراءات الأعمال المرتبطة بها.<br>■ تنفيذ تدابير الصمود اللازمة، التي تتناسب مع الاستخدام المقصود لكل جهاز؛ مع مراعاة المكونات الأخرى المرتبطة بنظام إنترنت الأشياء، أو الخدمة أو الجهاز.<br>■ ضمان كون وظائف الأمن السيبراني الأساسية لأجهزة إنترنت الأشياء وخدماتها؛ قادرة على العمل محليًا، في حال انقطاع التيار أو الشبكة، والعودة إلى الحال المرغوبة بعد الانقطاع. |
| 2-1-3 | على الأجهزة الطرفية، وخاصة أجهزة البوابة؛ أن تكون قادرة على تطبيق متطلبات الأمن السيبراني، عبر شبكات وبروتوكولات الاتصال حتى في حال انقطاع/تعطيل الاتصال بالشبكة الرئيسية. |

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

| | |
|---|---|
| 1-4 | الأمن السيبراني المتعلق بالأطراف الخارجية |
| الهدف | ضمان حماية أصول الجهة من مخاطر الأمن السيبراني في برمجيات ومكونات أجهزة إنترنت الأشياء التي تم شراؤها أو تشغيلها من قبل أطراف خارجية. |
| الإرشادات | |
| 1-1-4 | تحديد متطلبات الأمن السيبراني لإنترنت الأشياء ضمن العقود مع الموردين، ومقدمي الخدمات من الأطراف الخارجية، وتوثيقها واعتمادها وتطبيقها ومراجعتها دورياً. |
| 2-1-4 | الطلب من الشركات المصنعة، ومقدمي الخدمات لمنتجات إنترنت الأشياء وخدماتها، إثبات قدرات الأمن السيبراني في منتجاتهم و/أو خدماتهم. |
| 3-1-4 | الطلب من المطورين والمصنعين، تقديم قائمة بمكونات الأجهزة، والبرمجيات الموجودة في حزمة أجهزة إنترنت الأشياء؛ لمساعدة الجهة في فهم مخاطر الأمن السيبراني وإدارتها بشكل أفضل وتصحيح أي ثغرات أمنية معروفة على الفور. |
| 4-1-4 | تحديد أنظمة المعلومات، والمكونات، والخدمات، ذات العلاقة بإنترنت الأشياء المقدمة من قبل الموردين، ومقدمي الخدمات من الأطراف الخارجية لإدراجها في التقييم العام للمخاطر، وإجراءات التقليل من المخاطر. |
| 5-1-4 | تنفيذ أنشطة التحقق من خلال عمليات التدقيق، والاختبارات، والتأكد من شهادات البرمجيات؛ للتأكد من أن جميع المكونات المقدمة من الأطراف الخارجية في أجهزة إنترنت الأشياء؛ متوافقة مع سياسات الأمن السيبراني للجهة والمتطلبات الموضحة في العقود. |
| 6-1-4 | مراجعة إجراءات معالجة مخاطر الأمن السيبراني، وتدابير الأمن السيبراني لإنترنت الأشياء ذات العلاقة، بالموردين ومقدمي الخدمات من الأطراف الخارجية؛ لرصد أي إجراء غير مصرح به. |
| 2-4 | الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة |
| الهدف | ضمان تنفيذ متطلبات الأمن السيبراني لخدمات الحوسبة السحابية المستخدمة في أجهزة إنترنت الأشياء. |
| الإرشادات | |
| 1-2-4 | تحديد متطلبات الأمن السيبراني لخدمات إنترنت الأشياء السحابية المستضافة داخلياً في الجهة أو بشكل خاص والعمل على توثيقها واعتمادها وتطبيقها، بالإضافة إلى خدمات الحوسبة السحابية الأخرى المستخدمة خصيصاً لأجهزة إنترنت الأشياء، وتضمين ضوابط الأمن السيبراني للحوسبة السحابية (CCC) ومراجعتها دورياً. |
| 2-2-4 | وضع سياسات لإدارة التصاريح والصلاحيات والتحقق والتشفير وتقنياتها المناسبة لتأمين أجهزة إنترنت الأشياء التي تتفاعل مع خدمات الحوسبة السحابية المستضافة داخلياً/الخاصة و/أو الخدمات السحابية الأخرى التي تُستخدم خصيصاً لأجهزة إنترنت الأشياء. |
| 3-2-4 | 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. |

| | |
|---|---|
| 4-2-4 | 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 العامة للجهة. |
| 5-2-4 | تضمين أحكاماً خاصة بالحصول على البيانات المخزنة في المنصات السحابية بصياغة مقروءة لجميع الموردين، في حالة خروج مقدم خدمات الحوسبة السحابية و/أو مقدم الخدمات المدارة (المخطط أو غير المخطط) من اتفاقية تقديم خدمات الحوسبة السحابية في الاتفاقيات التعاقدية مع مقدمي خدمات الحوسبة السحابية و/أو مقدمي الخدمات المُدارة. |

# 7. ملاحق

## ملحق (أ): مصطلحات وتعريفات

يوضح الجدول (2) 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. |
| **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. |
| **إنترنت الأشياء Internet of Things** | يشير مصطلح إنترنت الأشياء الى الحساسات و الأجهزة ("الأشياء") المتصلة بالإنترنت و/أو الشبكات الأخرى والتي تضيف قيمة بناءً على البيانات؛ مثل تسهيل المهام. وتدعم تقنية إنترنت الأشياء العديد من حالات الاستخدام بما في ذلك المنازل الذكية والمدن الذكية والرعاية الصحية الذكية والسيارات الذكية. |
| **التصميم الآمن 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. |
| **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 2 : مصطلحات وتعريفات

## 7.1 ملحق (ب): قائمة الاختصارات

يوضح الجدول (3) أدناه، معنى الاختصارات التي ورد ذكرها في هذه الإرشادات.

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

جدول 3: قائمة الاختصارات