UNITED ARAB EMIRATES
MINISTRY OF CABINET AFFAIRS
PRIME MINISTER'S OFFICE

الإمارات العربية المتحدة
وزارة شؤون مجلس الوزراء
مكتب رئاسة مجلس الوزراء

السياسة الوطنية لأمن إنترنت الأشياء

الإصدار 0.3

مايو 2023

تنبيه

اعتُمدت هذه الوثيقة ووافق مجلس الوزراء في دولة الإمارات العربية المتحدة عليها، وهي ملكية حصرية وخاصة للمجلس الأمن السيبراني.

ويحتفظ مجلس الأمن السيبراني بحقه في تعديل، أو إضافة، أو حذف أي بند أو قسم من هذه السياسة.

لا يُمكن استخدام هذه الوثيقة أو أي جزءٍ منها دون الحصول على الموافقة الخطية المسبقة من مجلس الأمن السيبراني.

ضوابط الإصدار

الإصدار	0.1
التاريخ:	21 فبراير 2022
جهة الإعداد:	مجلس الأمن السبراني
التعديل:	المسودة الأولية

الإصدار	0.2
التاريخ:	08 مارس 2022
جهة الإعداد:	مجلس الأمن السبراني
التعديل:	التحديثات وفقاً للجلسة المنعقدة بتاريخ 24 فبراير 2022 مع هيئة أبوظبي الرقمية

الإصدار	0.3
التاريخ:	10 مايو 2022
جهة الإعداد:	مجلس الأمن السبراني
التعديل:	التحديثات حسب مراجعة الملاحظات بشأن مسودة الوثيقة ضمن الإصدار الثاني

	جهة المراجعة	جهة الموافقة
المسمى الوظيفي:	xxxxxxxxx	xxxxxxxxx
الاسم:	xxxxxxxxx	xxxxxxxxx
التوقيع:	xxxxxxxxx	xxxxxxxxx
التاريخ:	xxxxxxxxx	xxxxxxxxx

جدول المحتويات

جدول المحتويات

جدول المحتويات

جدول المحتويات

القسم 1

المقدّمة

المقدّمة

أصبحت الأجهزة المتصلة بالإنترنت مؤخراً بالغة الأهمية في حياتنا اليومية، ابتداءً من أجهزة تتبع النشاط البدني، ومروراً بأجهزة تنظيم ضربات القلب وكذلك السيارات، ووصولاً إلى أنظمة التحكّم المستخدمة لتوصيل المياه والكهرباء إلى منازلنا. وفي حقيقة الأمر، تساهم هذه الأجهزة في تمكين الاتصال السلس بين الأفراد والشبكات والخدمات المادية. وقد أصبحت هذه الأجهزة تستخدم بوتيرة متزايدة في جمع بيانات القياس أو تنفيذ العمليات والإجراءات دون التدخل البشري، معلنة انطلاق الثورة الصناعية الرابعة.

وفي الوقت الذي نواصل فيه دمج اتصالات الشبكات في البنية التحتية الحيوية لمجتمعنا، فإن هناك العديد من العمليات الحيوية المهمة التي كانت تُنفّذ يدوياً ومن خلال العزل المادي (وبذلك كانت تتمتع بقدر من الحصانة ضد الهجمات السيبرانية المعادية) أصبحت اليوم معرضة للمخاطر والتهديدات السيبرانية في ظل ما أنتجته التكنولوجيا من مستشعرات وأجهزة ذكية، وأجهزة المدن الذكية، وأنظمة النقل، والأجهزة الأوتوماتيكية، والروبوتات والأجهزة الطبية، وغيرها من المكونات الصناعية. وتُعد المخاطر الناتجة عن منظومة إنترنت الأشياء على خصوصية المستهلك والانقطاع المحتمل في خدمات البنية التحتية الحيوية مخاطر جسيمة وتتطلب اعتماد أسلوب ونهج شامل مع الاستمرار في دعم وتحسين الاتصال والأتمتة الذكية.

وضع مجلس الأمن السيبراني هذه السياسة لحماية استخدام واعتماد وتطبيق مبادرة إنترنت الأشياء، بما يتماشى مع الأولوية الوطنية لدولة الإمارات العربية المتحدة بأن تصبح رائدة عالمية في مجال الأمن السيبراني، كما ستساعد هذه السياسة في تحسين الوضع الأمني للمؤسسات والأفراد الذين يستخدمون منتجات وحلول إنترنت الأشياء داخل الدولة.

1.1 الهدف

تسعى هذه السياسة إلى تعزيز مكانة دولة الإمارات العربية المتحدة في مجال أمن إنترنت الأشياء من خلال التركيز على مبادئ تأمين منظومة إنترنت الأشياء ومعالجة التحديات التي تواجهها في مجال التكنولوجيا الناشئة. وستوفّر أيضاً إرشادات لمنظومة إنترنت الأشياء في الدولة وتعرف متطلبات أمن إنترنت الأشياء وتحدّد الجهات المسؤولة عن الإشراف على تشريعات أمن إنترنت الأشياء وإنفاذها.

وستساعد هذه السياسة في التأكد من التزام مقدّمي خدمات إنترنت الأشياء بتلبية مجموعة من المتطلبات الأمنية، والتأكد من توفير مستوى حماية لجميع مستخدمي إنترنت الأشياء سواء عند شراء الخدمات أو استخدامها. وتهدف هذه السياسة أيضاً إلى الحرص على تفادي الآثار السلبية المحتملة التي يُمكن أن تنتج عن تطبيقها، مثل: تثبيط الاستثمار وإعاقة نمو منظومة إنترنت الأشياء بسبب المتطلبات الصارمة للغاية.

1.2 النطاق ومدى قابلية التطبيق

لا شك أن تعزيز مكانة دولة الإمارات العربية المتحدة في أمن إنترنت الأشياء يقتضي دراسة جميع أجهزة ونطاقات إنترنت الأشياء. وتطبّق هذه السياسة على جميع الأجهزة والنطاقات ضمن جميع القطاعات في الدولة بما يتضمن، على سبيل المثال لا الحصر:

منظومة إنترنت الأشياء

الشبكة التي تربط الأجهزة التي تجمع البيانات وتشاركها وتعالجها عبر الإنترنت. ويُمكن أن تتراوح بين الأجهزة الاستهلاكية الشائعة، مثل: الساعات الذكية والأجهزة المنزلية الذكية وصولاً إلى الآلات الثقيلة ومعدات التصنيع. ومن الأمثلة عليها: الشبكة المنزلية الذكية التي تراقب الوقت من اليوم أو تستشعر وقت غروب الشمس وتغلق الستائر تلقائياً وتضيء الأنوار في المنزل، حيث أن هذا المثال البسيط يستخدم المستشعرات والأضواء الذكية والشبكات والحوسبة السحابية والمحركات لإكمال مهمتها.

أجهزة إنترنت الأشياء الصناعية

شبكة من الأجهزة المترابطة التي تربط بين المعدات الصناعية والمستشعرات للسماح بالأتمتة في جميع أنحاء المنشأة الصناعية. ويشير مصطلح إنترنت الأشياء الصناعي بصورة أساسية إلى الإطار الصناعي الذي يربط أدوات البرامج بين مختلف الآلات أو الأجهزة. وتصنّف أجهزة إنترنت الأشياء الصناعية من الروبوتات الصناعية المعقدة إلى المستشعرات البيئية الدقيقة. وعلى وجه العموم، تنفّذ الشركات مشاريع إنترنت الأشياء الصناعية لتحقيق كفاءة التكلفة الداخلية. ومن التطبيقات الأكثر استخداماً لإنترنت الأشياء الصناعية العدادات الذكية والشبكات الذكية والمصانع الذكية، وما شابه ذلك.

1.2 النطاق ومدى قابلية التطبيق

أجهزة إنترنت الأشياء للمدن الذكية

المستشعرات وأجهزة إنترنت الأشياء المستخدمة لجمع البيانات وتحليلها لتحسين الكفاءة التشغيلية للمدينة. وبفضل إنترنت الأشياء، تتحوّل المدن التقليدية إلى مدن ذكية. تندمج المستشعرات والبيانات والوصلات في المدينة الذكية لتطوير التقنيات الرقمية وأنظمة الاتصالات التي تعمل على تحسين العمليات في المدينة. ويُمكن للمدن الذكية الاستفادة من أجهزة إنترنت الأشياء والتقنيات الذكية في مجال السلامة العامة والأمن، وإدارة المياه والنفايات والنقل والتحكّم بتلوث الهواء، وأنظمة إدارة المباني، وما إلى ذلك.

أجهزة إنترنت الأشياء الطبية

منظومة الأجهزة الطبية المتصلة بالإنترنت وأطر الأجهزة وتطبيقات البرامج التي تربط تكنولوجيا المعلومات الصحية بالأطباء والمرضى. يوفّر إنترنت الأشياء الطبية للأجهزة اللاسلكية والبعيدة اتصالاً آمناً لمعالجة البيانات الطبية بسلاسة ومرونة عبر الإنترنت. فعلى سبيل المثال: يُمكن تصنيف أنظمة مراقبة ضغط الدم عن بُعد ومراقبة سرعة نبضات القلب عبر الإنترنت، وأنظمة مراقبة المرضى ضمن أجهزة إنترنت الأشياء الطبية.

المركبات المتصلة

تستخدم المركبات المتصلة أجهزة ومستشعرات إنترنت الأشياء المستخدمة للقيادة الذكية والفعّالة. وتدمج هذه المركبات مع تقنية إنترنت الأشياء، حيث تسمح هذه التقنية للسيارة بالارتباط بالأجهزة المجاورة من خلال الشبكات اللاسلكية لنقل البيانات في كلا الاتجاهين (اتصال ثنائي الاتجاه) مع المركبات الأخرى والأجهزة المحمولة والتقاطعات في المدينة. ويُمكن تصنيف السيارة ذاتية القيادة أو المركبة الآلية المسيّرة ضمن المركبات المتصلة.

1.2 النطاق ومدى قابلية التطبيق

تطبّق هذه السياسة على الجهات التالية العاملة في مجال أجهزة وخدمات إنترنت الأشياء داخل دولة الإمارات العربية المتحدة، بما يتضمن على سبيل المثال لا الحصر:

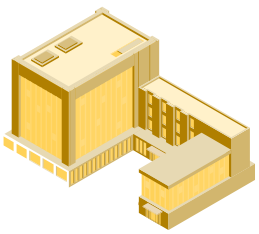
مستهلكو إنترنت الأشياء: مستهلكو إنترنت الأشياء هم المستخدمون النهائيون الذين يقومون بشراء واستخدام أجهزة أو أنظمة إنترنت الأشياء الجاهزة سواءً في القطاع الصناعي أو للاستخدام الشخصي. ويصنّف مستهلكو إنترنت الأشياء على النحو التالي، بناءً على قابلية تطبيق هذه السياسة:

الجهات المعنية بالبنية التحتية للمعلومات الحيوية

تطبّق سياسة أمن إنترنت الأشياء على جميع الجهات المعنية بالبنية التحتية للمعلومات الحيوية في دولة الإمارات العربية المتحدة، والتي تستخدم خدمات إنترنت الأشياء أو تخطط للحصول عليها والاستفادة منها. ويُرجى الرجوع إلى سياسة البنى التحتية للمعلومات الحيوية لدولة الإمارات العربية المتحدة للاطلاع على قائمة مفصّلة لقطاعات البنية التحتية للمعلومات الحيوية.

الجهات الحكومية

تطبّق سياسة أمن إنترنت الأشياء على جميع الجهات الحكومية في دولة الإمارات العربية المتحدة والتي تستخدم خدمات إنترنت الأشياء أو تخطط للحصول عليها والاستفادة منها.



الجهات الأخرى

لا تطبّق سياسة أمن إنترنت الأشياء على الجهات والمؤسسات الأخرى التي تستخدم خدمات إنترنت الأشياء أو تخطط للحصول عليها في الإمارات العربية المتحدة، إلّا أنها تُعتبر بمثابة دليل إرشادي لها.

الأفراد

لا تُعتبر سياسة أمن إنترنت الأشياء إلزامية على الأفراد الذين يستخدمون خدمات إنترنت الأشياء أو يخططون للحصول عليها في دولة الإمارات العربية المتحدة، إلّا أنها تُعتبر بمثابة دليل إرشادي لهم.

1.2 النطاق ومدى قابلية التطبيق

مقدّمو خدمات إنترنت الأشياء: تُعتبر سياسة أمن إنترنت الأشياء ملزمة لجميع مقدّمي خدمات إنترنت الأشياء والمطورين والمنفذين الذين يقدّمون خدمات إنترنت الأشياء في دولة الإمارات العربية المتحدة.

الشركات المصنّعة لإنترنت الأشياء: من المُوصى التزام الشركات المصنّعة لأجهزة إنترنت الأشياء بالمتطلبات المنصوص عليها في هذه السياسة إذا كانت ترغب بتصنيع أو بيع أجهزة إنترنت الأشياء داخل الدولة.

1.3 دورة حياة الاعتماد

يحدّد الإطار الوطني لحوكمة الأمن السيبراني نهجاً متكاملاً ومشتركاً لإدارة واعتماد الأمن السيبراني على مستوى الجهة، ومستوى القطاع، وعلى المستوى الوطني. ولذلك حدّد الإطار دورة واضحة تمكن من فهم وتقييم وتطبيق ومراقبة وتعزيز التعاون في مجال الأمن السيبراني داخل دولة الإمارات العربية المتحدة. وتضمن دورة الحياة هذه التطوير المستمر لقدرات الأمن السيبراني في الدولة من خلال توفير متطلبات محدّدة ومدارة ومعتمدة على نحوٍ جيد فيما يتعلق بالتقنيات الناشئة، مثل: إنترنت الأشياء.

فهم مدى تعقيد التقنيات المتصلة بالشبكة، وتزايد الاعتماد على البنية التحتية للمعلومات الحيوية الأخرى، والمحركات الاقتصادية، والمشهد العام للتهديدات داخل الدولة.

تقييم المخاطر التي تتعرض لها أجهزة وعمليات وخدمات إنترنت الأشياء، وتحديد مخاطر الاختراق أو الفشل المحتمل، وتحديد الأثر النسبي، واختيار الضوابط للتخفيف من حدة المخاطر.

تنفيذ ضوابط الأمن المحدّدة في المراحل الأولى من تحديد المتطلبات وتصميم حالة الاستخدام وتصميم هندسة التكنولوجيا وتطوير البرمجيات والإنتاج والعمليات.

مراقبة ومراجعة أداء وفاعلية الضوابط الأمنية المطبّقة.

التعاون لضمان التحسين المستمر للعمليات والخدمات والضوابط الأمنية.

1.4 مبادئ أمن إنترنت الأشياء

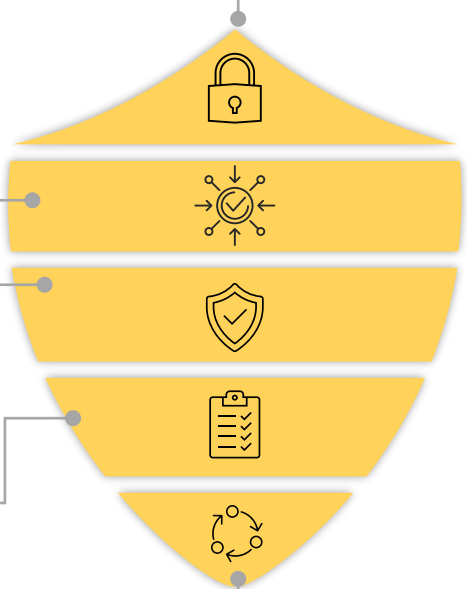
وُضعت مبادئ أمن إنترنت الأشياء الخمسة لتوفير العناصر الأساسية لصنّاع القرار فيما يتعلق باعتماد تكنولوجيا إنترنت الأشياء وتطبيقاتها وعملياتها في دولة الإمارات العربية المتحدة، حيث أنها تساعد مستهلكي إنترنت الأشياء ومقدّمي خدمات إنترنت الأشياء في اتخاذ قرارات الشراء والتشغيل بما يتماشى مع السياسات المفصّلة في هذه الوثيقة.

الأمان والخصوصية من خلال التصميم

يُستخدم الأجهزة المعتمدة، وأنظمة التشغيل المصممة خصيصًا، بالإضافة إلى الخدمات المُدارة من مقدّمي خدمات المعترف بهم، والموارد الماهرة لدعم تطوير التطبيقات الآمنة لإنترنت الأشياء والاستفادة منها وتشغيلها.

تحديد أولويات الأمان على أساس الأثر

تؤخذ التبعات المحتملة لانقطاع الخدمة أو الخرق أو الأنشطة الخبيثة التي يتعرض لها المستهلك بالاعتبار عند وضع وتحديد الجهود الأمنية وتكليف المسؤوليات للتخفيف من التبعات الوخيمة التي تنتج عنها.



الدفاع القوي

أُعد نهج شامل للأمن يشتمل على تفعيل الدفاعات متعددة الطبقات ضد تهديدات الأمن السيبراني في تصميم تطبيقات إنترنت الأشياء والمنظومة الخاصة بها.

إرشادات حول أفضل الممارسات

يُستفاد من أفضل الممارسات العالمية لتوفير الأمان وتعزيز كفاءات الامتثال.

منظومة تعاونية وشفافة

تُشارك المعلومات حول الثغرات الأمنية والمعلومات الاستخبارية علناً بين الشركات المصنعة ومقدّمي الخدمات والمستهلكين الصناعيين والجهات الرقابية بحيث يؤدي ذلك إلى زيادة مستوى الوعي.

1.5 الموافقة على الاستثناءات

يُحتمل أن يمنح مجلس الأمن السيبراني استثناء على السياسة في ظل ظروف خاصة.

تُراجع الاستثناءات على أساس كل حالة على حدة، حيث لا يُمكن ضمان الموافقة عليها.

2

القسم
مستهلكو
إنترنت الأشياء

يوضّح القسم التالي نطاقات السياسة الرئيسية منها والفرعية المطبّقة على مستهلكي إنترنت الأشياء في دولة الإمارات العربية المتحدة. وتركّز النطاقات الفرعية للسياسة تركيزاً أكبر على الأهداف وبيانات السياسة

2.1 حوكمة إنترنت الأشياء

2.1.1 إطار الحوكمة

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تأسيس القيادة والحوكمة لبدء ودعم تنفيذ متطلبات أمن إنترنت الأشياء.

بيانات السياسة

2.1.1.1 يجب على مستهلكي إنترنت الأشياء اعتماد نموذج حوكمة شامل لإدارة ومراقبة مكونات وخدمات إنترنت الأشياء المستخدمة في المنظومة ذات الصلة.

2.1.1.2 يجب على مستهلكي إنترنت الأشياء وضع استراتيجية وخطة لإدارة وتنفيذ ومراقبة أجهزة وخدمات إنترنت الأشياء، بالإضافة إلى فهم الأدوار والمسؤوليات الفردية.

2.1.1.3 يجب على مستهلكي إنترنت الأشياء التأكد من اطلاع وفهم مقدّمي خدمات إنترنت الأشياء والجهات المشغّلة والمستخدمين المشاركين في إدارة وتنفيذ ومراقبة أجهزة وخدمات إنترنت الأشياء لأدوارهم ومسؤولياتهم.

2.1 حوكمة إنترنت الأشياء

2.1.2 إدارة المخاطر

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تحديد ومعالجة المخاطر المتعلقة بالخصوصية وأمن إنترنت الأشياء على نحوٍ استباقي في الوقت المناسب.

بيانات السياسة

2.1.2.1 يجب إعداد وتنفيذ برنامج قوي ومستمر لإدارة المخاطر لإعداد منظومة إنترنت الأشياء ضمن نظام تقييم المخاطر.

2.1.2.2 يجب إجراء تقييمات المخاطر المتعلقة بأمان وخصوصية إنترنت الأشياء لتحليل الأثر على البيانات أو الأصول المستضافة في منظومة إنترنت الأشياء.

2.1 حوكمة إنترنت الأشياء

2.1.3 التوعية والتدريب

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تعزيز وعي الموظفين بالتهديدات والثغرات الأمنية الناشئة عن إنترنت الأشياء من خلال إخضاعهم لتدريبات مكثفة.

بيانات السياسة

2.1.3.1 يجب وضع خطة توعية وتدريب لتوفير تدريب متخصّص في مجال أمن إنترنت الأشياء لجميع الأفراد (الموظفين، والمقاولين، وموظفي الجهات الخارجية) لإدارة وتنفيذ ومراقبة أجهزة أو خدمات إنترنت الأشياء أو كليهما.

2.1.3.2 يجب تصميم التدريبات الخاصة بأمن إنترنت الأشياء على النحو المناسب يتوافق مع أدوار ومسؤوليات الموظفين.

2.1 حوكمة إنترنت الأشياء

2.1.4 أمن الجهات الخارجية

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تقليل احتمالية حدوث إخفاقات تشغيلية وخروقات لأمن البيانات من أي جهة خارجية.

بيانات السياسة

2.1.4.1 يجب وضع وتنفيذ سياسات أمان الجهات الخارجية لتسهيل تنفيذ الضوابط ذات الصلة والتأكد من التزام الجهات الخارجية المعنية بسياسات أمن إنترنت الأشياء الخاصة بالمؤسسة.

2.1.4.2 يجب إبرام اتفاقية عدم الإفصاح عن المعلومات، واتفاقيات مستوى الخدمة والاتفاقيات التعاقدية الموثّقة، بما يتضمن جميع متطلبات أمن إنترنت الأشياء والتوفّر والخصوصية بما يتماشى مع جميع المعايير والقوانين واللوائح المعمول بها والاتفاق عليها بوضوح.

2.1.4.3 تُمنح إمكانية وصول الجهات الخارجية إلى الطبقات المهمة من أجهزة إنترنت الأشياء بناءً على مبدأ منح أقل الامتيازات لفترة زمنية محدّدة، ويجب مراجعتها دورياً وتعديلها عند اللزوم.

2.1 حوكمة إنترنت الأشياء

2.1.5 الامتثال

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان التنفيذ الفعّال لضوابط أمن إنترنت الأشياء.

بيانات السياسة

2.1.5.1 يجب أن تتوافق حلول إنترنت الأشياء مع اللوائح المحلية والوطنية والدولية المعمول بها وأفضل الممارسات من خلال الحفاظ على برنامج إدارة الامتثال والتقييمات الدورية.

2.1.5.2 يجب أن تُطبَّق قوانين سيادة البيانات المعتمدة لدى دولة الإمارات العربية المتحدة على البيانات الحساسة أثناء جميع عمليات ومراحل التخزين والنقل والمعالجة.

2.1.5.3 ضمان الامتثال بمعايير الأمن السيبراني الصادر من مجلس الأمن السيبراني بقرار مجلس الوزراء رقم (8/8و) لسنة 2021

2.1.5.4 ضمان تطبيق المعايير والسياسات المعتمدة والمطبقة في هيئة تنظيم الاتصالات والحكومة الرقمية (TDRA) لتعزيز الأمن السيبراني

2.1.5.5 يجب الالتزام بالمعايير والسياسات المعتمدة والمطبقة من قبل الجهات والقطاعات المختصة بعمل القائمين على هذه التقنيات.

2.1.5.6 تطبيق معايير الأمن السيبراني الصادر من المنظمة الدولية للمعايير (27001 و 27002)

2.2 أمن البيانات

2.2.1 خصوصية البيانات والحوكمة

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

حماية سرية أو مصداقية أو توفّر البيانات أو جميعها (بما فيها المعلومات التعريفية الشخصية) التي يجري جمعها أو تخزينها أو معالجتها أو نقلها من أو إلى جهاز إنترنت الأشياء.

بيانات السياسة

2.2.1.1 يجب تحديد العمليات والإجراءات الفنية وتوثيقها وتنفيذها لتصنيف البيانات على أساس الحساسية وذلك بهدف توثيق المواقع المادية للبيانات.

2.2.1.2 يجب تزويد المستهلكين بمعلومات واضحة وشفافة حول كيفية استخدام بياناتهم، وعن الجهات التي تستخدمها، والغرض الذي تستخدمها لأجله، لكل جهاز وخدمة من أجهزة وخدمات إنترنت الأشياء.

2.2.1.3 يجب أن يكون مستهلك منتجات وخدمات إنترنت الأشياء قادراً على ممارسة حقوقه فيما يتعلق بالمعلومات، والبيانات، وصلاحية الوصول إليها، وقدرته على مسحها، وتصحيحها، وقابلية نقلها، وتقييد عمليات المعالجة والاعتراض على المعالجة، وكذلك حقه في عدم تقييمها بناءً على المعالجة الآلية.

2.2.1.4 يجب على مستهلك منتجات وخدمات إنترنت الأشياء حماية سرية أو مصداقية أو توفّر البيانات أو جميعها، بما فيها معلومات التعريف الشخصية التي يجري جمعها أو تخزينها أو معالجتها أو نقلها من أو إلى جهاز إنترنت الأشياء.

2.2.1.5 يجب إبرام اتفاقية تعاقدية لتقييد أي استخدام أو إفشاء غير مصرح به للمعلومات أو البيانات السرية.

2.2.1.6 يجب وضع السياسات والإجراءات لحماية الموقع المادي أو المنطقي للبيانات ومنع أي عمليات الجمع غير مصرح بها للبيانات التشخيصية أو البيانات المستخدمة لأغراض التحليل.

2.2 أمن البيانات

2.2.2 التشفير

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان الاستخدام المناسب لقدرات التشفير لغرض تأمين البيانات المخزنة ومعاملات البيانات وتبادلها بين أجهزة إنترنت الأشياء.

بيانات السياسة

2.2.2.1 يجب تحديد جذر الثقة على المستوى المؤسسي، وهو عبارة عن مجموعة من سياسات وإجراءات التشفير التي تتحكّم في كيفية تأمين المعرفات، والتطبيقات، والاتصالات بشكل مشفر. يساعد هذا النموذج في ضمان تأمين جميع الرسائل من خلال التسلسل الهرمي للتشفير.

2.2.2.2 يجب استخدام مفتاح خاص بالجذر، سواء كان متماثلًا أو غير متماثل، للتوقيع رقمياً على المفاتيح الأخرى المستخدمة في التسلسل الهرمي.

2.2.2.3 يجب تطبيق نهج التشفير القائم على المخاطر لتأمين جميع الاتصالات ضد التهديدات التقليدية والكمية.

2.2 أمن البيانات

2.2.3 الاتصالات الآمنة والموثوق بها

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان سرية (خصوصية) وتكامل وتوفّر ومصداقية المعلومات أثناء نقلها عبر الشبكات أو أثناء تخزينها على تطبيق إنترنت الأشياء أو في الحوسبة السحابية.

بيانات السياسة

2.2.3.1 تأسيس إدارة آمنة للجلسة، ونظراً لوجود اتصالات مختلفة في أنظمة إنترنت الأشياء، بالإضافة إلى العديد من الجلسات التي يتم إنشاؤها، فمن الضروري تنفيذ جلسات آمنة من أجل ضمان أمن الاتصالات.

2.2.3.2 وضع سياسات وإجراءات إدارة الجلسة لجلسات الاتصالات المختلفة والتأكد من إدماج ضوابط المصادقة على الجلسات وضوابط انتهاء صلاحية الجلسات في السياسات والإجراءات بهدف منع فقدان الجلسة أو انتهاكها.

2.2.3.3 يجب توظيف بروتوكولات الاتصال الآمن باستخدام القنوات المشفرة وحماية السلامة والاتصالات المصادق عليها لمشاركة المعلومات بين أنظمة إنترنت الأشياء. يجب استخدام تقنيات التشفير المثبتة لحماية البيانات الموجودة على أي من أنظمة إنترنت الأشياء والبنية التحتية الأساسية.

2.3 إدارة الهوية والوصول

2.3.1 التحكّم بالوصول

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

منع الوصول غير المصرح به وأي عمليات لتعديل أو تغيير الموارد والتطبيقات والبيانات المؤسسية أثناء استخدام خدمات إنترنت الأشياء.

بيانات السياسة

2.3.1.1 وضع وتطبيق سياسة إدارة صلاحيات الوصول المبنية على مفهوم الحد الأدنى من الامتيازات، مع المعرفات الفريدة للموارد المطلوبة فقط، ومع وضع الأسس والضوابط المناسبة لتفعيل عمليات المساءلة وعدم الإنكار.

2.3.1.2 وضع وتنفيذ آليات مصادقة قوية لأنظمة إنترنت الأشياء، وفرض وجوب استخدام كلمات مرور قوية، وأرقام تعريف شخصية قوية، مع إمكانية تفعيل المصادقة متعددة العوامل في حلول إنترنت الأشياء.

2.3.1.3 يجب مصادقة جميع أشكال الوصول إلى أنظمة إنترنت الأشياء باستخدام آليات مصادقة مركزية. ويجب تخزين أي بيانات اعتماد بأمان داخل الخدمات وعلى الأجهزة. ولن تُقبل بيانات الاعتماد المشفرة في برامج الجهاز.

2.3.1.4 يجب التحكّم بالوصول إلى موارد النظام وإدارتها طوال دورات حياتها، مما يقلل من فرص تعرضها للهجمات الخبيثة.

2.3.1.5 تنفيذ مراقبة الوصول ومراجعة الوصول في أنظمة إنترنت الأشياء (والبنية التحتية الأساسية الأخرى) للتأكد من أن النظام يتحقّق من أن المستخدمين والتطبيقات لديهم الأذونات المناسبة والنظر في نشر ضوابط تعويضية إضافية في حالة تغيير الموظفين.

2.3.1.6 التأكد من توافق كلمات المرور مع سياسة تعقيد كلمة المرور الداخلية ومعايير الصناعة، وطلب تعيين كلمة مرور جديدة بعد فترة محدّدة.

2.3 إدارة الهوية والوصول

2.3.2 الوصول المادي

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان حماية بيئة إنترنت الأشياء من الوصول المادي غير المصرح به.

بيانات السياسة

2.3.2.1 يجب توفير الوصول المادي للمستخدمين ممن لديهم حاجات مبررة من الناحية التجارية، مع منح التفويض المناسب وإخضاعهم للمراقبة.

2.3.2.2 يجب توفير جميع حركات الوصول المادي والمنطقي فقط للمستخدمين الذين تم فحصهم على النحو المناسب، بما يتضمن التحقّق من الخلفية وتنفيذ عمليات العناية الواجبة بشأنهم.

2.3.2.3 يجب حظر الوصول المادي والتحكّم به باستخدام أنظمة الحماية ضد العبث والاحتواء والأقفال الميكانيكية أو الإلكترونية.

2.4 إدارة الحوادث

2.4.1 إدارة الحوادث

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تقليل أثر المخاطر والتحديات الأمنية في بيئة إنترنت الأشياء.

بيانات السياسة

2.4.1.1 وضع وتطبيق استراتيجية وخطة قوية وناجحة للاستجابة للحوادث بهدف احتواء الحوادث والتعافي منها مع ضمان الحد الأدنى من الأثر على سير الأعمال.

2.4.1.2 يجب تصنيف الحوادث على أساس الأثر التجاري أو التشغيلي على المؤسسة.

2.4.1.3 يجب وضع أدلة إدارة الحوادث المعمول بها مع تفصيل التهديدات والأثر المحتمل وأنشطة الاحتواء والتعافي وتحديدها على نحوٍ مسبق.

2.4 إدارة الحوادث

2.4.2 الاستجابة للحوادث

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

احتواء وتقليل الآثار الناتجة عن الحوادث الأمنية.

بيانات السياسة

2.4.2.1 يجب تقييم فاعلية خطة الاستجابة للحوادث الأمنية والفريق المكلف بها دورياً.

2.4.2.2 يجب استخدام تحليل ما بعد الحادث، ووضع الدروس المستفادة منه لتعزيز استراتيجية وخطة الاستجابة للحوادث باستمرار.

2.4.2.3 يجب إعداد حلول وخدمات إنترنت الأشياء بحيث تكون في وضع مرن أثناء وقوع أي أحداث غير متوقعة.

2.4 إدارة الحوادث

2.4.3 إعداد التقارير حول الحوادث

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان الإبلاغ عن الحوادث الأمنية ضمن إطار زمني مناسب وباستخدام صيغ مقبولة.

بيانات السياسة

2.4.3.1 يجب رفع تقارير حول أي عيوب أو اختلالات ترصد إلى فريق إدارة الحوادث المعني ضمن المؤسسة.

2.4.3.2 يجب الكشف عن الحوادث الأمنية والإبلاغ عنها للسلطات المحلية والوطنية ذات الصلة خلال أُطر زمنية محدّدة، ويجب أن يكون التقرير أو عملية الاتصال مدعومة بجميع الوثائق الضرورية.

2.4 إدارة الحوادث

2.4.4 التحقيقات الجنائية بشأن إنترنت الأشياء

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تحديد النوايا وراء حدوث الخروقات الأمنية، بالإضافة إلى تحديد نطاقها فيما يتعلق بأجهزة إنترنت الأشياء وتنفيذ عمليات التحري اللازمة بالخصوص.

بيانات السياسة

2.4.4.1 تحديد الموارد اللازمة لتقديم الدعم في التحليل الجنائي لإنترنت الأشياء.

2.4.4.2 استخدام طرق فعّالة أو عملية آلية لتتبع البيانات على أجهزة إنترنت الأشياء وفي الشبكة وفي الحوسبة السحابية.

2.4 إدارة الحوادث

2.4.5 إدارة الثغرات الأمنية

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

دعم تحديد الثغرات الأمنية وتصنيفها وترتيب أولويات التعامل معها ومعالجتها والتخفيف من أثرها في بيئة إنترنت الأشياء.

بيانات السياسة

2.4.5.1 يجب تحديد وتنفيذ عملية إدارة شاملة للثغرات الأمنية من أجل التحديد الاستباقي للثغرات ومعالجتها في الوقت المناسب.

2.4.5.2 يجب تقييم الثغرات الأمنية في أجهزة إنترنت الأشياء وحلولها، والبيئات المطبّقة فيها دورياً لتحديدها على نحوٍ استباقي ولإبلاغ الجهات المعنية بشأنها.

2.4.5.3 يجب تحديث وتنفيذ التصحيحات لأنظمة إنترنت الأشياء وتطبيقاتها بانتظام لتقليل احتمال تعرضها للتهديدات.

2.4.5.4 يجب إجراء اختبار اختراق مستقل بالاعتماد على جهات خارجية دورياً أو بعد حدوث أي تغييرات كبيرة في النظام ضمن البيئة الخاضعة للرقابة.

2.4.5.5 يجب تطبيق قدرات التحليل الذكي للمخاطر لرصد وتقييم التهديدات الأمنية ضمن أنظمة إنترنت الأشياء.

2.5 مرونة إنترنت الأشياء

2.5.1 النسخ الاحتياطية الآمنة

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان توفّر المعلومات والتخفيف من آثار الحوادث.

بيانات السياسة

2.5.1.1 يجب على مستهلكي إنترنت الأشياء إجراء نسخ احتياطية دورياً لبيانات المستخدم والإعدادات، بالإضافة إلى إجراء اختبار استعادة النسخ الاحتياطية.

2.5.1.2 يتعين على مستهلكي أنترنت الأشياء حفظ وتوثيق بيانات النسخ الاحتياطية باستخدام أنظمه تكنولوجية متقدمة مع استخدام أساليب التشفير المعتمدة بهذا الشأن

2.5.1.3 تحديد وتوفير صلاحيات الولوج والإطلاع ونقل واستعادة النسخ الاحتياطية من قبل المخولين ضمن المؤسسة وفق الأدوار والمسؤوليات المعتمدة والمصرح لها.

2.5.1.4 يجب على مستهلكي أنترنت الأشياء اتباع الضوابط الأمنية الخاصة بتخزين ونقل واستعادة النسخ الاحتياطية لضمان سرية وسلامة البيانات.

2.5.1.5 يجب على مستهلكي انترنت الأشياء إجراء اختبار سلامة النسخ الإحتياطية بشكل دوري لضمان وجود نسخة إحتياطية بديلة في حال وقوع أي حدث مني او كارثة طبيعية.

2.5 مرونة إنترنت الأشياء

2.5.2 التعافي من الكوارث

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان توفّر الموارد والمعلومات على قدرٍ كبير كجزء من الجهود المتواصلة، بالإضافة إلى العمل على تقليل أثر انقطاع الخدمات والحوادث.

بيانات السياسة

2.5.2.1 يجب على مستهلكي إنترنت الأشياء تقييم حلول وخدمات إنترنت الأشياء ومتطلبات توفّر المعلومات لضمان استمرارية الخدمات.

2.5.2.2 يجب على مستهلكي إنترنت الأشياء وضع خطة للتعافي من الكوارث لضمان استمرارية عمليات إنترنت الأشياء.

2.5.2.3 يجب على مستهلكي أنترنت الأشياء متابعة و تحديث خطط التعافي و استمرارية الاعمال بشكل دوري لضمان تطبيق و الامتثال الافضل للمعايير الدولية و الوطنية.

2.6 إدارة الأجهزة

2.6.1 إدارة الأصول

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

الحفاظ على مخزون وإدارة أصول إنترنت الأشياء عبر دورة حياتها، بما يتضمن الأجهزة والبرامج.

بيانات السياسة

2.6.1.1 يجب على مستهلكي إنترنت الأشياء وضع إجراءات إدارة الأصول والحفاظ عليها لأنظمة إنترنت الأشياء الحساسة والمهمة.

2.6.1.2 يجب الحفاظ على مخزون أجهزة إنترنت الأشياء وتحديثه بانتظام وذلك فيما يتعلق بمجموعة الأجهزة المتصلة والبرامج وإصدارات البرامج الثابتة المرتبطة به.

2.6.1.3 يجب على مستهلكي إنترنت الأشياء وضع إجراءات لضمان تطبيق إجراءات الصيانة اللازمة في الوقت المناسب لأجهزة إنترنت الأشياء، واستبدال أو التخلص الآمن من أجهزة إنترنت الأشياء التي انتهى عمرها الافتراضي أو التي أصبحت خارج الخدمة.

2.6 إدارة الأجهزة

2.6.2 أمن التطبيقات

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تطبيق الضوابط الأمنية اللازمة في التطبيقات التي تتفاعل مع أجهزة إنترنت الأشياء والمكونات ذات الصلة.

بيانات السياسة

2.6.2.1 يجب تهيئة مكونات حلول إنترنت الأشياء مثل التطبيقات والبرمجيات الوسيطة وواجهات برمجة التطبيقات والأجهزة للمصادقة الآمنة وتبادل المعلومات عبر القنوات المشفرة.

2.6.2.2 يجب تنفيذ التطبيقات باستخدام عناصر التوفّر وعناصر التحكّم الأمنية الشاملة عبر جميع حلول إنترنت الأشياء، كما يجب فرض قواعد التحكّم بالوصول على طبقة خدمات موثوقة بها.

2.6.2.3 يجب استخدام بوابة آمنة ومخصّصة لإدماج البيانات ومعالجتها داخل شبكات إنترنت الأشياء.

2.6 إدارة الأجهزة

2.6.3 أمن الأجهزة

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

حماية بيئة إنترنت الأشياء أثناء دورة الحياة التشغيلية للجهاز.

بيانات السياسة

2.6.3.1 يجب تثبيت أجهزة ومستشعرات إنترنت الأشياء وتهيئتها بأمان لحماية الأجهزة من العبث أو الوصول غير المصرح به.

2.6.3.2 يجب عند إدارة أو استخدام أجهزة إنترنت الأشياء عن بُعد استخدام قنوات مشفرة ومصادق عليها، مع تمكين وتفعيل آليات سجلات الأمان.

2.6.3.3 يجب توثيق وتنفيذ استراتيجية إدارة الأجهزة وضمان التحديثات الدورية والصيانة الدورية لحماية أجهزة إنترنت الأشياء.

2.6.3.4 يجب تنفيذ تصحيحات الأمان والتحديثات من مصادر موثوقة دورياً في وضع آمن ومحمي من الفشل، بما يتضمن التوافق مع تكوينات الأمان المحدّدة في إصدارات البرامج الثابتة السابقة.

2.6.3.5 يجب اختبار جميع التصحيحات والتحديثات وتقييمها من حيث المخاطر ومدى الأثر قبل تطبيقها عبر جميع أجهزة أو أنظمة إنترنت الأشي

2.6.3.6 يجب تطبيق التدابير التعويضية على الأجهزة التي وصلت إلى نهاية عمرها الافتراضي.

2.7 أمن الشبكات

2.7.1 إدارة الشبكات

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان حماية مكونات شبكة إنترنت الأشياء والمنظومات ذات الصلة.

بيانات السياسة

2.7.1.1 يجب تأمين شبكات إنترنت الأشياء باستخدام منافذ وبروتوكولات آمنة مع تمكين عمليات وإجراءات المصادقة والتشفير.

2.7.1.2 يجب مراعاة ضوابط الأمن وإمكانية التشغيل التفاعلي عبر شبكات التوجيه المختلفة.

2.7.1.3 يجب فصل شبكات إنترنت الأشياء عن شبكة المؤسسة، كما يجب تقسيمها إلى شرائح متناهية الصغر للتحكّم الدقيق بالوصول إليها.

2.7.1.4 يجب تقييد ومراقبة تبادل المعلومات وإدارة البنية التحتية لأجهزة وتطبيقات إنترنت الأشياء.

2.7.1.5 يجب إيقاف الخدمات الشبكية والبروتوكولات والمنافذ غير المستخدمة والافتراضية.

2.7.1.6 يجب أن تطبّق إدارة حلول إنترنت الأشياء عبر شبكة منفصلة ومستقلة.

2.7.1.7 يجب أن يستخدم جهاز إنترنت الأشياء الخاص بالمستهلك أفضل إمكانيات التشفير لتمكين الاتصالات الآمنة.

2.8 بيانات الدخول والمراقبة الأمنية

2.8.1 سجل التدقيق

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تتبع وتسجيل الأنشطة والأحداث في بيئة إنترنت الأشياء.

بيانات السياسة

2.8.1.1 يجب تمكين أجهزة إنترنت الأشياء والأنظمة وسجلات التطبيقات ومراقبتها في الوقت الفعلي، حيثما كان ذلك ممكناً من الناحية الفنية.

2.8.1.2 يجب مراقبة أجهزة إنترنت الأشياء والأنظمة وسجلات التطبيقات وحمايتها من الوصول أو الاتصال أو أي تغيير غير مصرح به للإعدادات.

2.8.1.3 يجب مراجعة وتدقيق ضوابط الأمان لأجهزة وأنظمة وتطبيقات إنترنت الأشياء دورياً.

2.8 بيانات الدخول والمراقبة الأمنية

2.8.2 المراقبة

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تحديد وكشف ومعالجة الوصول والاستخدام غير المصرح به للأنظمة والمعلومات.

بيانات السياسة

2.8.2.1 يجب ربط أجهزة وأنظمة إنترنت الأشياء وسجلات التطبيق وتحليلها ومراجعتها لتحديد أي تهديد أمني أو نشاط ضار.

2.8.2.2 يجب إجراء مراقبة منتظمة لسلوك الجهاز لاكتشاف البرامج الضارة واكتشاف الأخطاء المتعلقة بالسلامة.

2.8.2.3 يجب الاحتفاظ بأجهزة إنترنت الأشياء والأنظمة وسجلات التطبيقات بأمان وبما يلبي متطلبات سياسة الاحتفاظ المطبّقة لدى الجهة ومتطلبات القوانين واللوائح المعمول بها.

3

القسم

مقدّمو خدمات إنترنت الأشياء

يوضّح القسم التالي نطاقات السياسة الرئيسية منها والفرعية المطبّقة على مستهلكي إنترنت الأشياء في دولة الإمارات العربية المتحدة. وتركّز النطاقات الفرعية للسياسة تركيزاً أكبر على الأهداف وبيانات السياسة

3.1 حوكمة إنترنت الأشياء

3.1.1 إطار الحوكمة

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تأسيس القيادة والحوكمة لبدء ودعم تنفيذ متطلبات أمن إنترنت الأشياء.

بيانات السياسة

3.1.1.1 يجب وضع استراتيجية وبرنامج أمن إنترنت الأشياء وتحديد هيكل الحوكمة والنموذج التشغيلي لأمن إنترنت الأشياء بما يتوافق مع المعايير والقوانين واللوائح السارية.

3.1.1.2 يجب التأكد من اطلاع وفهم مقدّمي خدمات إنترنت الأشياء والجهات المشغّلة والمستخدمين المشاركين في إدارة وتنفيذ ومراقبة أجهزة وخدمات إنترنت الأشياء لأدوارهم ومسؤولياتهم.

3.1.1.3 يجب الحرص على سرية البيانات الشخصية الخاصة بمستخدمي التقنيات ومُلاك الآلات والأجهزة المرتبطة، مع ضمان تشفيرها وضمان سلامتها وحمايتها .(CIA)

3.1.1.4 يجب إنشاء سجل يحتوي على التقنيات والأجهزة والآلات المستخدمة لتقنيات انترنت الأشياء لضمان التحديث المستمر للبيانات.

3.1 حوكمة إنترنت الأشياء

3.1.2 إدارة المخاطر

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تحديد ومعالجة المخاطر المتعلقة بالخصوصية وأمن إنترنت الأشياء على نحوٍ استباقي في الوقت المناسب.

بيانات السياسة

3.1.2.1 يجب إعداد وتنفيذ برنامج قوي ومستمر لإدارة المخاطر لإعداد منظومة إنترنت الأشياء ضمن نظام تقييم المخاطر.

3.1.2.2 يجب إجراء تقييمات المخاطر المتعلقة بأمان وخصوصية إنترنت الأشياء لتحليل الأثر على البيانات أو الأصول المستضافة في منظومة إنترنت الأشياء.

3.1 حوكمة إنترنت الأشياء

3.1.3 التوعية والتدريب

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تعزيز وعي الموظفين بالتهديدات والثغرات الأمنية الناشئة عن إنترنت الأشياء من خلال إخضاعهم لتدريبات مكثفة.

بيانات السياسة

3.1.3.1 يجب وضع خطة توعية وتدريب لتوفير تدريب متخصّص في مجال أمن إنترنت الأشياء لجميع الأفراد (الموظفين، والمقاولين، وموظفي الجهات الخارجية) لإدارة وتنفيذ ومراقبة أجهزة أو خدمات إنترنت الأشياء أو كليهما.

3.1.3.2 يجب تصميم التدريبات الخاصة بأمن إنترنت الأشياء على النحو المناسب يتوافق مع أدوار ومسؤوليات الموظفين.

3.1 حوكمة إنترنت الأشياء

3.1.4 أمن الجهات الخارجية

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تقليل احتمالية حدوث إخفاقات تشغيلية وخروقات لأمن البيانات من أي جهة خارجية.

بيانات السياسة

3.1.4.1 يجب وضع وتنفيذ سياسات أمان الجهات الخارجية لتسهيل تنفيذ الضوابط ذات الصلة والتأكد من التزام الجهات الخارجية المعنية بسياسات أمن إنترنت الأشياء الخاصة بالمؤسسة.

3.1.4.2 يجب إبرام اتفاقية عدم الإفصاح عن المعلومات، واتفاقيات مستوى الخدمة والاتفاقيات التعاقدية الموثّقة، بما يتضمن جميع متطلبات أمن إنترنت الأشياء والتوفّر والخصوصية بما يتماشى مع جميع المعايير والقوانين واللوائح المعمول بها والاتفاق عليها بوضوح، وذلك عند شراء خدمات إنترنت الأشياء.

3.1.4.3 يجب وضع وتنفيذ خطة إدارة سلسلة التوريد لحماية سلامة سلسلة التوريد. ويجب أن تتضمن الخطة الأطر الأمنية وإدارة المخاطر والمتطلبات التعاقدية.

3.1 حوكمة إنترنت الأشياء

3.1.5 الامتثال

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان التنفيذ الفعّال لضوابط أمن إنترنت الأشياء.

بيانات السياسة

3.1.5.1 يجب أن تتوافق حلول إنترنت الأشياء مع اللوائح المحلية والوطنية والدولية المعمول بها وأفضل الممارسات من خلال الحفاظ على برنامج إدارة الامتثال والتقييمات الدورية.

3.1.5.2 يجب أن تُطبَّق قوانين سيادة البيانات المعتمدة لدى دولة الإمارات العربية المتحدة على البيانات الحساسة أثناء جميع عمليات ومراحل التخزين والنقل والمعالجة.

3.1.5.3 ضمان الامتثال بمعايير الأمن السيبراني الصادر من مجلس الأمن السيبراني بقرار مجلس الوزراء رقم (8/8و) لسنة 2021

3.1.5.4 ضمان تطبيق المعايير والسياسات المعتمدة والمطبقة في هيئة تنظيم الاتصالات والحكومة الرقمية (TDRA) لتعزيز الأمن السيبراني

3.1.5.5 يجب الالتزام بالمعايير والسياسات المعتمدة والمطبقة من قبل الجهات والقطاعات المختصة بعمل القائمين على هذه التقنيات.

3.1.5.6 تطبيق معايير الأمن السيبراني الصادر من المنظمة الدولية للمعايير (27001 و 27002)

3.2 أمن البيانات

3.2.1 خصوصية البيانات والحوكمة

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

حماية سرية أو مصداقية أو توفّر البيانات أو جميعها (بما فيها المعلومات التعريفية الشخصية) التي يجري جمعها أو تخزينها أو معالجتها أو نقلها من أو إلى جهاز إنترنت الأشياء.

بيانات السياسة

3.2.1.1 يجب منع الوصول إلى البيانات أو العبث بها عندما تكون في حالة التخزين أو أثناء نقلها وبما قد يسبب انكشاف معلومات حساسة أو السماح بالتلاعب أو تعطيل عمليات أجهزة إنترنت الأشياء.

3.2.1.2 يجب التعهد بالالتزام في حماية البيانات وبما يلبي المتطلبات المنصوص عليها في اللوائح المعتمدة عند إعداد وتقديم أجهزة وخدمات إنترنت الأشياء.

3.2.1.3 يجب مراقبة وتحليل نشاط أجهزة إنترنت الأشياء للبحث عن أي حوادث قد تكون مرتبطة بأمن البيانات.

3.2.1.4 يجب تزويد المستهلكين بجميع الحقوق المنصوص عليها وفقاً لقانون خصوصية البيانات المعمول به، وذلك للحفاظ على خصوصيتهم من خلال وضع الإعدادات الآمنة للأجهزة وبهدف تحقيق فاعلية الخدمات المقدّمة.

3.2.1.5 أثناء التعامل مع بيانات المستخدم الحساسة، يتعهد مقدّمو خدمات إنترنت الأشياء بالحفاظ على حماية سرية أو مصداقية أو توفّر البيانات أو جميعها (بما فيها المعلومات التعريفية الشخصية) التي يجري جمعها أو تخزينها أو معالجتها أو نقلها من أو إلى جهاز إنترنت الأشياء.

3.2.1.6 الإقرار على السياسات والإجراءات والموافقة بشأنها وفقاً للاتفاقية التعاقدية لتقييد أي استخدام أو إفشاء غير مصرح به لبيانات المستخدم ومعلوماته السرية. الحفاظ على الموقع المادي أو المنطقي لبيانات المستخدم وفقاً للاتفاقية الموقعة، وذلك لمنع أي عمليات جمع غير مصرح بها للبيانات التشخيصية أو المستخدمة لأغراض التحليل.

3.2 أمن البيانات

3.2.2 التشفير

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان الاستخدام المناسب لقدرات التشفير لغرض تأمين البيانات المخزنة ومعاملات البيانات وتبادلها بين أجهزة إنترنت الأشياء.

بيانات السياسة

3.2.2.1 يجب ضمان السرية أو المصداقية أو سلامة البيانات والمعلومات أو جميعها (بما يتضمن رسائل التحكّم)، أثناء النقل وفي حالة التخزين من خلال الاختيار المناسب لخوارزميات التشفير والمفاتيح القوية وتعطيل البروتوكولات غير الآمنة.

3.2.2.2 يجب على مقدّم الخدمات أن يحرص على توافق الأجهزة مع الأساليب الأمنية وأساليب التشفير البسيط.

3.2.2.3 يجب أن تطبّق أساليب التشفير وأفضل الممارسات التي تعتمدها الجهات المصنعة على النحو المناسب والملائم على أجهزة وأنظمة إنترنت الأشياء.

3.2.2.4 يجب تطبيق الواجهات الشبكية الآمنة لأنظمة إنترنت الأشياء باستخدام أساليب التشفير والمصادقة والتفويض.

3.2.2.5 يجب استخدام أحدث وأفضل خوارزميات التشفير (Encryption algorithms) المعيارية والمعتمدة.

3.2 أمن البيانات

3.2.3 الاتصالات الآمنة والموثوق بها

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان عدم اختراق الاتصالات باستخدام القنوات المشفرة، بالإضافة إلى حماية السلامة والاتصال المصادق عليه لمشاركة المعلومات بين أنظمة إنترنت الأشياء.

بيانات السياسة

3.2.3.1 يجب أن تكون أجهزة إنترنت الأشياء مقيّدة بدلاً من أن تكون اختيارية ومتساهلة في عمليات الاتصال وينبغي فتح وتشغيل المنافذ المخصّصة فقط للاتصال المختار.

3.2.3.2 يجب تطبيق الواجهات الشبكية الآمنة لأنظمة إنترنت الأشياء باستخدام أساليب للتحقّق من المصادقة والتفويض.

3.2.3.3 فرض سياسات وإجراءات إدارة الجلسة، لجلسات الاتصالات المختلفة وإيجاد ضوابط تحكّم لإنهاء الجلسة ولمصادقتها، وذلك لتأمين الاتصال من وقوع حالات القرصنة للجلسة وفقاً لمتطلبات المستهلك.

3.2.3.4 فرض بروتوكولات الاتصال بما فيها القنوات المشفرة وحماية السلامة ومصادقة الاتصالات لتأمين عمليات الاتصال بين أجهزة وأنظمة إنترنت الأشياء وفقاً لمتطلبات المستهلك.

3.3 إدارة الهوية والوصول

3.3.1 التحكّم بالوصول

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

منع الوصول غير المصرح به وأي عمليات لتعديل أو تغيير الموارد والتطبيقات والبيانات المؤسسية أثناء استخدام خدمات إنترنت الأشياء.

بيانات السياسة

3.3.1.1 وضع وتطبيق سياسة إدارة صلاحيات الوصول المبنية على مفهوم الحد الأدنى من الامتيازات، مع المعرفات الفريدة للموارد المطلوبة فقط، ومع وضع الأسس والضوابط المناسبة لتفعيل عمليات المساءلة وعدم الإنكار.

3.3.1.2 يجب مصادقة جميع أشكال الوصول إلى أنظمة إنترنت الأشياء باستخدام آليات مصادقة مركزية. ويجب تخزين أي بيانات اعتماد بأمان داخل الخدمات وعلى الأجهزة. ولن تُقبل بيانات الاعتماد المشفرة في برامج الجهاز.

3.3.1.3 يجب التحكّم بالوصول إلى موارد النظام وإدارتها طوال دورات حياتها، مما يقلل من فرص تعرضها للهجمات الخبيثة.

3.3.1.4 يجب على مقدّمي خدمات إنترنت الأشياء والمسؤولين تمكين آلية تعمل على توفير خاصية تغيير الاسم وكلمة المرور الافتراضية قبل ربط الجهاز مع الشبكة.

3.3 إدارة الهوية والوصول

3.3.2 الوصول المادي

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان حماية بيئة إنترنت الأشياء من الوصول المادي غير المصرح به.

بيانات السياسة

3.3.2.1 يجب توفير الوصول المادي للمستخدمين ممن لديهم حاجات مبررة من الناحية التجارية، مع منح التفويض المناسب وإخضاعهم للمراقبة.

3.3.2.2 يجب توفير جميع حركات الوصول المادي والمنطقي فقط للمستخدمين الذين تم فحصهم على النحو المناسب، بما يتضمن التحقّق من الخلفية وتنفيذ عمليات العناية الواجبة بشأنهم.

3.3.2.3 يجب حظر الوصول المادي والتحكّم به باستخدام أنظمة الحماية ضد العبث والاحتواء والأقفال الميكانيكية أو الإلكترونية.

3.4 إدارة الحوادث

3.4.1 إدارة الحوادث

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تقليل أثر المشكلات الأمنية في بيئة إنترنت الأشياء.

بيانات السياسة

3.4.1.1 يجب على مقدّمي خدمات تطبيق استراتيجية وخطة قوية وناجحة للاستجابة للحوادث بهدف احتواء الحوادث والتعافي منها مع ضمان الحد الأدنى من الأثر على سير الأعمال والنشاطات التجارية وبما يلبي متطلبات الإطار الوطني والخطة الوطنية للاستجابة للحوادث.

3.4.1.2 يجب أن تستند إرشادات تصنيف الحوادث إلى الأثر التشغيلي أو التجاري على بيئة المستهلكين.

3.4.1.3 دعم المستهلكين في إعداد وتنفيذ أدلة إدارة الحوادث المعمول بها مع تفصيل التهديدات والأثر المحتمل وأنشطة الاحتواء والتعافي وتحديدها على نحوٍ مسبق

3.4 إدارة الحوادث

3.4.2 الاستجابة للحوادث

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

احتواء وتقليل الآثار الناتجة عن الحوادث الأمنية.

بيانات السياسة

3.4.2.1 يجب تقييم فاعلية خطة الاستجابة للحوادث الأمنية والفريق المكلف بها دورياً.

3.4.2.2 يجب استخدام تحليل ما بعد الحادث، ووضع الدروس المستفادة منه لتعزيز استراتيجية وخطة الاستجابة للحوادث باستمرار.

3.4.2.3 يجب إعداد حلول وخدمات إنترنت الأشياء بحيث تكون في وضع مرن أثناء وقوع أي أحداث غير متوقعة.

3.4 إدارة الحوادث

3.4.3 إعداد التقارير حول الحوادث

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان الإبلاغ عن الحوادث الأمنية ضمن إطار زمني مناسب وباستخدام صيغ مقبولة.

بيانات السياسة

3.4.3.1 يجب رفع تقارير حول أي عيوب أو اختلالات ترصد إلى فريق إدارة الحوادث المعني ضمن المؤسسة.

3.4.3.2 يجب على مقدّمي خدمات إنترنت الأشياء إرسال تقارير عن الحوادث بصورة عاجلة للمستهلك أو الجهة المتأثرة ضمن فترة زمنية محدّدة. ويجب على مقدّمي خدمات إنترنت الأشياء أيضاً إبلاغ المستهلك عن أي حوادث تتعلق بجهة خارجية مشتركة (حوادث تتعلق بسلسلة التوريد).

3.4 إدارة الحوادث

3.4.4 إدارة الثغرات الأمنية

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

دعم تحديد الثغرات الأمنية وتصنيفها وترتيب أولويات التعامل معها ومعالجتها والتخفيف من أثرها في بيئة إنترنت الأشياء.

بيانات السياسة

3.4.4.1 يجب تحديد وتنفيذ عمليات إدارة شاملة للثغرات الأمنية من أجل التحديد الاستباقي للثغرات ومعالجتها في الوقت المناسب.

3.4.4.2 يجب تقييم الثغرات الأمنية في أجهزة إنترنت الأشياء وحلولها، والبيئات المطبّقة فيها دورياً لتحديدها على نحوٍ استباقي ولإبلاغ الجهات المعنية بشأنها.

3.4.4.3 يجب تحديث وتنفيذ التصحيحات لأنظمة إنترنت الأشياء وتطبيقاتها بانتظام لتقليل احتمال تعرضها للتهديدات.

3.4.4.4 يجب إجراء اختبار اختراق مستقل بالاعتماد على جهات خارجية دورياً أو بعد حدوث أي تغييرات كبيرة في النظام ضمن البيئة الخاضعة للرقابة.

3.4.4.5 يجب تطبيق قدرات التحليل الذكي للمخاطر لرصد وتقييم التهديدات الأمنية ضمن أنظمة إنترنت الأشياء.

3.5 مرونة إنترنت الأشياء

3.5.1 مرونة خدمات إنترنت الأشياء

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان توفّر مكونات إنترنت الأشياء على قدرٍ كبير كجزء من الجهود المتواصلة، بالإضافة إلى العمل على تقليل أثر انقطاع الخدمات والحوادث.

بيانات السياسة

3.5.1.1 يجب أن يضمن مقدّمو خدمات إنترنت الأشياء إمكانية إجراء نسخ احتياطية لبيانات النظام بانتظام (بما يتضمن الإعدادات).

3.5.1.2 يجب أن تحتوي أجهزة وخدمات إنترنت الأشياء على قدرات مدمجة تحافظ على أداء عملها وتشغيل خصائصها الأساسية داخلياً في حالة حدوث انقطاع في الاتصالات.

3.5.1.3 يجب على حلول وخدمات إنترنت الأشياء امتلاك القدرة على استرجاع المعلومات بطريقة آمنة في حالة التعطل.

3.5.1.4 يجب أن تزوّد أنظمة إنترنت الأشياء بآليات تعمل على التشخيص والإصلاح الذاتي للتعافي من فشل الأداء والأعطال، أو حالة وجود اختراق. وإذا تعذّر إجراء إصلاح ذاتي أو آلي، يجب استخدام أساليب استرجاع يدوية للسماح لنظام إنترنت الأشياء بالرجوع إلى العمل بصورة آمنة.

3.6 إدارة الأجهزة

3.6.1 إدارة الأصول

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

إدارة أصول إنترنت الأشياء عبر دورة حياة اعتمادها، بما يتضمن الأجهزة والبرامج.

بيانات السياسة

3.6.1.1 يجب توفير ممارسات إدارة الأصول وضوابط الإعدادات لأنظمة المعلومات الرئيسية للمستهلكين.

3.6.1.2 يجب أن تطبّق إجراءات تركيب وصيانة أجهزة إنترنت الأشياء بالحد الأدنى من الخطوات والسماح للمستهلكين بإجراء الإعدادات بطريقة آمنة.

3.6.1.3 يجب وضع استراتيجية انتهاء مدة الصلاحية واتباعها بالنسبة لمنتجات إنترنت الأشياء، بالإضافة إلى الإقرار بشأن فترة انتهاء الدعم الأمني والتصحيحي.

3.6.1.4 يجب وضع الحلول الأمنية المثبتة، بما فيها بروتوكول الاتصالات وضوابط التشفير كأولوية بالنسبة لمنتجات إنترنت الأشياء، بدلاً من إيجاد حلول مخصّصة.

3.6 إدارة الأجهزة

3.6.2 أمن التطبيقات

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تطبيق الضوابط الأمنية اللازمة في التطبيقات التي تتفاعل مع أجهزة إنترنت الأشياء والمكونات ذات الصلة.

بيانات السياسة

3.6.2.1 يجب تطوير التطبيقات باستخدام إطار تطوير البرمجيات الآمنة مع الأخذ بعين الاعتبار جميع المتطلبات الأمنية، بما فيها ضبط الإعدادات الضرورية الأمنية والخاصة والمبنية على الموقع الجغرافي.

3.6.2.2 يجب أن تحظى التطبيقات بمنطق تشغيل آمن، وواجهة آمنة لعمليات إدخال وإخراج البيانات، بالإضافة إلى إمكانية تعقب الأحداث والأنشطة.

3.6.2.3 يجب استخدام بوابة آمنة ومخصّصة لإدماج البيانات ومعالجتها داخل شبكات إنترنت الأشياء.

3.6 إدارة الأجهزة

3.6.3 أمن الأجهزة

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

حماية بيئة إنترنت الأشياء أثناء دورة الحياة التشغيلية للجهاز.

بيانات السياسة

3.6.3.1 يجب مراعاة متطلبات الأمن والخصوصية تلقائياً عند تصميم أجهزة إنترنت الأشياء، ويتضمن ذلك وجود خصائص تخزين مشفرة وإرسال إشعارات للدخول غير المصرح به.

3.6.3.2 يجب تثبيت أجهزة ومستشعرات إنترنت الأشياء وتهيئتها بأمان لحماية الأجهزة من العبث أو الوصول غير المصرح به.

3.6.3.3 يجب أن تعمل أجهزة إنترنت الأشياء بطريقة آمنة بينما تعمل على حماية وسلامة مكونات الجهاز والبرامج. ويجب على تلك الأجهزة استخدام النظام وإدارة الاتصالات وتنفيذ البرمجية بأمان.

3.6.3.4 يجب أن تكون مكونات البرمجية في الأجهزة المتصلة بالإنترنت قابلة للتحديث بأمان. ويجب إتاحة خصائص التحديث وتطبيقاته للمستهلكين عند الحاجة. ويجب أن تكون الأجهزة المقيّدة، والتي لا يُمكن تحديثها بشكل مادي، قابلة للعزل والاستبدال.

3.7 أمن الشبكات

3.7.1 إدارة الشبكات

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

ضمان حماية مكونات شبكة إنترنت الأشياء.

بيانات السياسة

3.7.1.1 يجب تأمين شبكات إنترنت الأشياء باستخدام منافذ وبروتوكولات آمنة مع تمكين عمليات وإجراءات المصادقة والتشفير.

3.7.1.2 يجب مراعاة ضوابط الأمن وإمكانية التشغيل التفاعلي عبر شبكات التوجيه المختلفة.

3.7.1.3 يجب فصل شبكات إنترنت الأشياء عن شبكة المؤسسة، كما يجب تقسيمها إلى شرائح متناهية الصغر للتحكّم الدقيق بالوصول إليها.

3.7.1.4 يجب تقييد ومراقبة تبادل المعلومات وإدارة البنية التحتية لأجهزة وتطبيقات إنترنت الأشياء.

3.7.1.5 يجب إيقاف الخدمات الشبكية والبروتوكولات والمنافذ غير المستخدمة والافتراضية.

3.7.1.6 يجب أن تطبّق إدارة حلول إنترنت الأشياء عبر شبكة منفصلة ومستقلة.

3.8 بيانات الدخول والمراقبة الأمنية

3.8.1 سجل التدقيق

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	الرقابة	التعاون

هدف السياسة

تتبع وتسجيل الأنشطة والأحداث في بيئة إنترنت الأشياء.

بيانات السياسة

3.8.1.1 يجب تمكين البيانات القياسية لخدمات إنترنت الأشياء لكشف الخلل، وتسجيل وتشخيص دخول الأجهزة الطرفية.

3.8.1.2 يجب على الأجهزة الطرفية لإنترنت الأشياء تسجيل دخولها حسب سلوكها وتحميل السجل على الخدمات الموجودة على الخادم.

4

القسم

التنفيذ

التنفيذ

يجب قراءة هذه السياسة بالتوافق مع إطار ضوابط أمن إنترنت الأشياء في الملحق 6.5 والذي يوفّر بيانات التحكّم التي تدعم متطلبات السياسة.

سيعمل مجلس الأمن السيبراني مع الجهات المنظّمة للقطاعات والجهات المسؤولة داخل كل إمارة لضمان الامتثال لمتطلبات هذه السياسة.

يُتوقع من مستهلكي ومقدّمي الخدمات تنفيذ تقييمات ذاتية للامتثال لمتطلبات السياسة هذه وإبلاغ السلطات المعنية سنوياً أو كما هو مطلوب.

يُعد الأمن والتعليم والتوعية والتواصل من العناصر المهمة لإلهام التغيير اللازم بهدف النجاح في تعزيز إنترنت الأشياء. وسيتواصل مجلس الأمن السيبراني مع المشاركين لتعزيز إنترنت الأشياء كونه أولوية مؤسسية وطنية. ووُضعت العمليات والإجراءات والحلول لدعم جمع المعلومات وتحليلها ونشرها واستخدامها عبر الحدود المؤسسية، لذلك سيعمل مجلس الأمن السيبراني على رفع مستوى الوعي بما يبني فهماً أساسياً وثقة بين المشاركين. وبالإضافة إلى ذلك، سيعمل المجلس مع الجهات المعنية المشاركة للاعتراف بجهود المؤسسات التي تساهم بمعلومات ينتج عنها حلول وروابط سيبرانية مبتكرة بين مصادر المعلومات المختلفة بما يعزز مرونة الفضاء السيبراني لدولة الإمارات العربية المتحدة.

5

القسم

مراقبة الأداء

مراقبة الأداء

تحدّد السياسة الوطنية لأمن إنترنت الأشياء تدابير رصد وتقييم التقدّم المحرز نحو الأهداف التالية:

- تعزيز الشفافية والإدارة الفعّالة لأجهزة إنترنت الأشياء
- تقديم إرشادات للتحسين واتخاذ خطوات التدخل اللازمة عند اللزوم.
- قياس مدى نجاح مقدّمي الخدمات والمستخدمين في تطبيق المتطلبات الأمنية لإنترنت الأشياء.

القسم 6

الملاحق

6.1 الوثائق المرجعية

معايير وسياسات دولة الإمارات العربية المتحدة

يوضّح الجدول التالي معايير وسياسات دولة الإمارات العربية المتحدة التي يستند إليها عند تحديد متطلبات الأمن المنصوص عليها في هذه السياسة.

الهيئة/ الجهة	الوثيقة
مجلس الأمن السيبراني	قانون ضمان أمن المعلومات في دولة الإمارات العربية المتحدة.
هيئة تنظيم الاتصالات والحكومة الرقمية	سياسة تنظيم إنترنت الأشياء
هيئة تنظيم الاتصالات والحكومة الرقمية	الإجراءات التنظيمية لإنترنت الأشياء
مركز دبي للأمن الإلكتروني	أمن إنترنت الأشياء
مركز دبي للأمن الإلكتروني	معايير أمن إنترنت الأشياء
دائرة الصحة	المعيار الأمني لإنترنت الأشياء الطبية في قطاع الرعاية الصحية

6.1 الوثائق المرجعية

المعايير الدولية

يوضّح الجدول التالي المصادر الدولية المشار إليها في هذه الوثيقة.

الهيئة/ الجهة	الوثيقة
المعهد الوطني للمعايير والتقنية	800-213 - إرشادات الأمن السيبراني لأجهزة إنترنت الأشياء للحكومة الفيدرالية
المعهد الوطني للمعايير والتقنية	8228 - اعتبارات لإدارة إنترنت الأشياء الأمن السيبراني والمخاطر المتعلقة بالخصوصية
المعهد الوطني للمعايير والتقنية	8259 - أنشطة الأمن السيبراني التأسيسي للشركات المصنّعة لأجهزة إنترنت الأشياء
المعهد الوطني للمعايير والتقنية	8259A - خط الأساس الرئيسي لقدرات الأمن السيبراني لأجهزة إنترنت الأشياء
ISO/IEC	27402 - أمن وخصوصية إنترنت الأشياء - المتطلبات الأساسية للأجهزة
ISO/IEC	21823-1 - إمكانية التشغيل التفاعلي لأنظمة إنترنت الأشياء
ISA/IEC	62443 - يحدّد المعيار القدرات الأمنية لمكونات نظام التحكّم
IEEE	P2413 - أنشطة المعايير في إنترنت الأشياء
IEEE	1451-99 - معيار مواءمة أجهزة وأنظمة إنترنت الأشياء
وكالة الاتحاد الأوروبي للأمن السيبراني	WP2017 - التوصيات الأساسية الأمنية لأجهزة إنترنت الأشياء
وكالة الاتحاد الأوروبي للأمن السيبراني	WP2018 - الممارسات الجيدة لأمن إنترنت الأشياء
وكالة الاتحاد الأوروبي للأمن السيبراني	WP2019 - الممارسات الجيدة لأمن إنترنت الأشياء

6.2 الاختصارات

الهيئة/ الجهة	الوثيقة
API	واجهة برمجة التطبيقات
CVE	الثغرات الأمنية والمخاطر الشائعة
DDoS	هجمات الحرمان من الخدمة الموزعة
FISMA	قانون تحديث أمن المعلومات
FOIA	قانون حرية المعلومات
ICS	أنظمة التحكّم الصناعية
IoT	إنترنت الأشياء
IP	بروتوكول الإنترنت
IR	تقرير الحوادث
IT	تكنولوجيا المعلومات
ITL	مختبر تكنولوجيا المعلومات
LTE	الجيل الرابع من شبكة الاتصالات المتنقلة
MAC	وحدة التحكّم بالوصول إلى الوسائط
NIST	المعهد الوطني للمعايير والتقنية
PII	المعلومات التعريفية الشخصية
ROM	ذاكرة للقراءة فقط
SBOM	قائمة مكونات البرمجية
SDK	أدوات تطوير البرامج
SP	الإصدار الخاص
SSDF	إطار تطوير البرامج الأمني
USB	الناقل التسلسلي العالمي
UWB	الشبكات عريضة النطاق
Wi-Fi	الشبكة اللاسلكية
SDLC	دورة حياة تطوير البرنامج

6.3 الأدوار والمسؤوليات

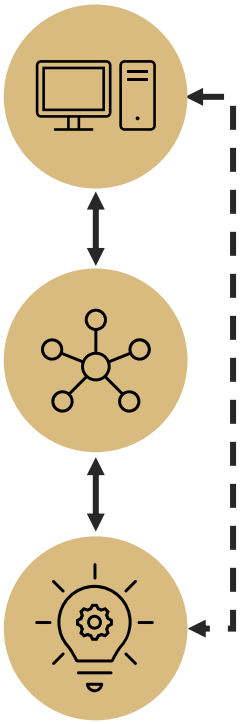
يحدّد الجدول أدناه الجهات المعنية الرئيسية وأدوارها ومسؤولياتها فيما يتعلق بهذه السياسة.

الجهات المعنية	الأدوار والمسؤوليات
مجلس الأمن السيبراني لدولة الإمارات العربية المتحدة	• بصفته الجهة المعنية والمسؤولة عن هذه الوثيقة، سيظلع مجلس الأمن السيبراني بما يلي: • إصدار سياسة أمن إنترنت الأشياء الوطنية ومراجعة الوثيقة دورياً للتأكد من صحتها وسريانها. • التنسيق مع الجهات المعنية لتوزيع هذه السياسة على القطاعات والجهات الحيوية. • الإشراف على تنفيذ الأحكام المنصوص عليها في السياسة والتأكد من الامتثال لها.
الجهات الحكومية وقطاعات البنى التحتية للمعلومات الحيوية الوطنية	• الامتثال للمتطلبات الموضّحة في سياسة أمن إنترنت الأشياء الوطنية. • تطبيق أحكام السياسة على الخدمات المعمول بها. • التحقّق من تلبية المتطلبات الواجبة وإجراء تقييمات المخاطر الموضّحة في هذه السياسة.
مقدّمو خدمات إنترنت الأشياء	• يجب على مقدّمي خدمات إنترنت الأشياء الامتثال لمتطلبات الأمن الموضّحة في هذه السياسة.
الأفراد	• لا يعتبر الأفراد ملزمين بالامتثال لمتطلبات الأمن الموضّحة في السياسة، إلّا أنه يوصى بالاستعانة بهذه السياسة كدليل إرشادي لهم في حال رغبتهم بشراء واستخدام خدمات إنترنت الأشياء في دولة الإمارات العربية المتحدة.
الشركات المصنّعة لأجهزة إنترنت الأشياء:	• من المُوصى التزام الشركات المصنّعة لأجهزة إنترنت الأشياء بالمتطلبات المنصوص عليها في هذه السياسة إذا كانت ترغب بتصنيع أو بيع أجهزة إنترنت الأشياء داخل الإمارات العربية المتحدة.
مستهلكو إنترنت الأشياء	• قد يختار هؤلاء المستخدمون الالتزام بمتطلبات الأمن المذكورة في السياسة لغايات تحسين وضعهم الأمني.

6.4 الخلاصة

6.4.1 وصف إنترنت الأشياء

استُمد تعريف مصطلح إنترنت الأشياء المستخدم في هذه السياسة من ورقة العمل الصادرة من معهد المهندسين الكهربائيين والإلكترونيين (IEEE) تحت عنوان "تعريف إنترنت الأشياء". فوفقاً للمعهد، فإن إنترنت الأشياء يتكون من اثنين من المكونات الرئيسية، وهما: (1) شبكة الإنترنت ذاتها، (2) الأجهزة شبه المستقلة ("الأشياء") التي تستفيد من قدرات الطاقة الحاسوبية والشبكات والاستشعار والتحويل في التطبيقات الفريدة بهدف استشعار العالم الحقيقي والتحكّم به. وبما أنها مبنية على نظام بروتوكول الإنترنت، فإن هذه الأجهزة تمتلك القدرة على الاتصال بالإنترنت أو تشغيلها على شبكات مستقلة غير متصلة بالإنترنت. وبالإضافة لذلك، فإن إنترنت الأشياء يشمل أيضاً الأدوات والبرامج والأنظمة (المنصات) التي تسمح بفهم السلوكيات وتحليل البيانات من هذه الأجهزة.



الأجهزة

تعدّ الأجهزة ضمن الشبكة بما يتيح معالجتها فردياً.

المنصة

تتصل الأجهزة ببعضها باستخدام منصة مشتركة، مثل: خدمات الحوسبة السحابية.

التحليل الذكي

يُمكن أن تؤدي الأجهزة وظائفها على نحوٍ ملائم، إما بمفردها أو مع أجهزة وتطبيقات أخرى، وذلك بناءً على البرمجة والمُدخلات الواردة من العالم الفعلي.

6.4 الخلاصة

6.4.2 وجهة نظر مستخدمي إنترنت الأشياء

في سبيل اتخاذ نهج تعاوني يهدف إلى الاستجابة للمخاطر المتعلقة بأجهزة إنترنت الأشياء وأنظمتها، فإن مجلس الأمن السيبراني لدولة الإمارات العربية المتحدة يأخذ وجهة نظر المستخدمين بشأن مخاطر أمن إنترنت الأشياء بعين الاعتبار وذلك لتعزيز الإرشادات والمتطلبات المنصوص عليها في هذه السياسة. وتُصنّف المخاطر الموضّحة في القسم أدناه إلى ثلاث مجموعات رئيسية للمستخدمين المسؤولين عن استخدام أجهزة إنترنت الأشياء، وهي:

- المستهلكون
- المؤسسات
- الحكومة

المستهلكون

عادةً ما يكون استخدام المستهلكين لأجهزة إنترنت الأشياء في منازلهم ومركباتهم ولوازمهم. ويُمكن أن تتسم هذه الاستخدامات بما يلي:

- أجهزة المشاركة ذات القدرة الحاسوبية المحدودة، مثل: الأجهزة المتصلة بالإنترنت أو أنظمة الأمن التي قد يستخدمها الأفراد أو المجموعات
- التحليلات الآلية للبيانات التي ينشئها المستخدم باستخدام التطبيقات المستندة إلى الحوسبة السحابية على أجهزة الشاشات الصغيرة، مثل: تتبع الأنشطة الحركية، ومن ثم استخدام تطبيق الهاتف المحمول لمراقبة التقدّم المُحرز من تلك الأنشطة
- الأجهزة المتصلة المستخدمة لتبادل بيانات المستخدم أو مراقبتها، مثل: الكاميرات المتصلة عبر بروتوكول الإنترنت. وغالباً، يُمكن لهذه الأجهزة نقل بعض المعلومات الحساسة.

6.4 الخلاصة

6.4.2 وجهة نظر مستخدمي إنترنت الأشياء

المؤسسات

تستفيد المؤسسات والشركات من إنترنت الأشياء لتحسين العمليات التجارية (الصيانة وسلسلة التوريد والمخزون) وتعزيز تجربة العملاء (التنفيذ، والبيع بالتجزئة). كما تستخدم حلولاً مبتكرة أخرى للتعامل مع العديد من التحديات التجارية التي تواجهها. وقد يشار إلى هذه التطوّرات أيضاً باسم الثورة الصناعية الرابعة القائمة على التكنولوجيا.

وتولي المؤسسات والشركات إلى حدٍ كبير اهتماماً بالمخاطر المتعلقة بالخصوصية الناتجة عن التهديدات ونقاط الضعف في بيئات إنترنت الأشياء، وهو ما يُعد تحدي آخر قد تواجهه المؤسسات، وهو إدارة إنترنت الأشياء والمخاطر الإلكترونية على مستوى المؤسسة.

- تعتمد عمليات المؤسسة اعتماداً كبيراً على توفّر البيانات وسلامتها، وبالتالي قد يكون لتلف البيانات تبعات وخيمة على المؤسسة. فعلى سبيل المثال: قد يتم اختراق الأجهزة الطبية لكشف المعلومات الحساسة للمريض، كما يُمكن استخدام هجمات القرصنة للتسبب في حجب الوصول وإلحاق الضرر بالسمعة.
- يُمكن تحسين القدرة على مواجهة التهديدات السيبرانية في بيئات إنترنت الأشياء، كما يُمكن أن تحدث الثغرات الأمنية عندما لا تُعالج تلك التهديدات السيبرانية على النحو المناسب. على سبيل المثال: يُمكن استخدام أجهزة إنترنت الأشياء لإنشاء شبكة الروبوتات للأجهزة التي تستخدم في هجمات الحرمان من الخدمة الموزعة.

6.4 الخلاصة

6.4.2 وجهة نظر مستخدمي إنترنت الأشياء

الحكومة

قد تكون استخدامات إنترنت الأشياء في الحكومة أكثر تنوعاً، ومنها في المؤسسات، وغالباً ما تُستخدم لتحسين الخدمات المقدّمة للمواطنين وتحسين جهود حماية البيئة (مثل: مراقبة العوامل البيئية وتقديم الخدمات الحكومية الإلكترونية).

تتشابه مخاطر أمن إنترنت الأشياء في الحكومة مع تلك التي تتعرض لها المؤسسات، إلّا أن هناك مخاوف إضافية لدى الحكومة والتي تتعلق بما يلي:

- الامتثال للحد الأدنى من متطلبات الأمن الأساسية وفقاً للمعايير المؤسسية وأفضل الممارسات.
- التهديدات المتزايدة التي تتعرض لها البنية التحتية الحيوية والهجمات من جهات التهديد التابعة لدول معينة.
- دورة حياة جهاز إنترنت الأشياء عندما يصل المنتج إلى نهاية عمره الافتراضي أو خروجه من الخدمة.

6.4 الخلاصة

6.4.3 الابتكار في إنترنت الأشياء

على الرغم من أن عالم إنترنت الأشياء قد شهد تطوّراً وإقبالاً كبيراً في السنوات القليلة الماضية، إلّا أن قدرات الأجهزة والحلول المبتكرة تتزايد باستمرار. ولا يزال إنترنت الأشياء في مراحله الأولى، ومع التقنيات الجديدة، مثل: شبكة الجيل الخامس (5G) والمعالجة المتطوّرة (قوة المعالجة على أجهزة إنترنت الأشياء)، فستشهد التطبيقات والابتكارات المستقبلية لإنترنت الأشياء تحسينات وتطورات كبيرة خلال السنوات القادمة. وفي ظل الثورة الصناعية الرابعة القائمة على التكنولوجيا، توجد هناك مخاطر أمنية متعددة أيضاً يجب أخذها بعين الاعتبار في المراحل الأولى من هذه الابتكارات. وعلى الرغم من أن هذه السياسة لا يُمكن أن تتناول جميع الجوانب المستقبلية لأمن إنترنت الأشياء، فإن الهدف يتمثّل في التطرق إلى بعض التغييرات الناشئة في مجال إنترنت الأشياء وبذل الجهود للاستعداد لما هو قادم.

وفيما يلي بعض التوجّهات التي نشهدها في تقنية إنترنت الأشياء والتكنولوجيا المحيطة بها:

- **الاتصال:** السماح باتصالات الشبكة في الوقت الفعلي وشبه الفعلي دون انقطاع
- **المنصات:** معالجة قابلية التوسّع والمسائل المتعلقة بالأمان مع استخدام نهج موحّد
- **البنى الموحّدة:** تمكين الأجهزة الموزّعة من الاندماج في الشبكات المتطوّرة والشبكات السحابية
- **تقنية دفتر الأستاذ الموزَّع:** استخدام تقنية البلوكتشين للمعاملات الآمنة على الأجهزة المتطورّة
- **الذكاء الاصطناعي:** تكامل الأجهزة والأنظمة التي تدعم الذكاء الاصطناعي في طبقات مختلفة من منظومة إنترنت الأشياء للسماح باتخاذ القرارات المستقلة.
- **الاتصال اللمسي:** نقل قوة الحوسبة إلى ما هو أبعد من الحوسبة السحابية أو حوسبة الحافة ليصل إلى الأجهزة نفسها.