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

الإمارات العربية المتحدة
وزارة شؤون مجلس الوزراء
مكتب رئاسة مجلس الوزراء

سياسة حماية البنية التحتية للمعلومات الحيوية

الإصدار 1.0

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 السيبراني
التعديل:	المسودة الأولية

الإصدار	0.2
التاريخ:	08 مارس 2022
جهة الإعداد:	مجلس الأمن السيبراني
التعديل:	التحديثات وفقاً للملاحظات الأولية

الإصدار	1.0
التاريخ:	30 أغسطس 2022
جهة الإعداد:	مجلس الأمن السيبراني
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

القسم 1

المقدّمة

المقدّمة

يُعد موضوع حماية البنى التحتية للمعلومات الحيوية أمراً غاية في التعقيد، كما أنه أيضاً على قدر كبير من الأهمية لجميع الدول، حيث تعتمد الدول جميعها على خدمات البنى التحتية الحيوية، مثل: تزويد الطاقة، والاتصالات، والأنظمة المالية، والخدمات الحكومية. وفي الوقت الذي تعتمد البنية التحتية الحيوية فيه على البنية التحتية للمعلومات التي تتكون من التكنولوجيا التشغيلية، والخدمات المبنية على تكنولوجيا المعلومات والاتصالات، وعلى التكنولوجيا المرتبطة أو المتصلة ببعضها، وذلك لتؤدي هذه البنى التحتية عملها على الوجه المطلوب. ومن الممكن أن يؤدي تعطيل أي من هذه البنى التحتية للمعلومات إلى تعريض الأمن والاستقرار الوطني للخطر، كما يؤثر تأثيراً كبيراً على النمو الاقتصادي، وعلى حياة الأفراد وأسلوب معيشتهم، وقد يكون له أثرٌ بعيد المدى أيضاً بسبب الترابط الوثيق بين منظومات هذه البنى التحتية. وفتحت عمليات التحوّل الرقمي الواسعة التي نُفّذت خلال الأعوام القليلة الماضية المجال أما حدوث مجموعة واسعة وكبيرة من الهجمات السيبرانية المعقدة، والتي تراوحت من الهجمات باستخدام البرمجيات الخبيثة، وهجمات القراصنة، وهجمات الجماعات الناشطة في مجال القرصنة، وصولاً إلى العمليات السيبرانية التي تنفذها الدول المعادية، وهي التي تُستخدم لتنفيذ الهجمات على البنية التحتية الحيوية الوطنية. ولذلك أصبح من الأهمية بمكان ولزاماً على معظم الدول وضع استراتيجيات فعّالة لحماية البنى التحتية للمعلومات الحيوية.

وضع المجلس هذه السياسة لضمان وضع معيار قياسي للمرونة السيبرانية للبنى التحتية للمعلومات الحيوية، وبما يتماشى مع الأولويات الوطنية لدولة الإمارات في أن تصبح دولة رائدة عالمية في مجال الأمن السيبراني، ولتطبيق هذه المعايير القياسية نحو الوصل إلى فضاء سيبراني مرن وآمن لبنيتها التحتية للمعلومات الحيوية.

1.1 الهدف

تهدف هذه السياسة إلى تعزيز قدرات الأمن السيبراني لدولة الإمارات العربية المتحدة، وذلك من خلال تحديد نهج متسق وقابل للتكرار لتعريف، وتقييم وإعداد ملف المخاطر الوطني عبر جميع البنى التحتية للمعلومات الحيوية.

كما ستوفّر هذه السياسة آلية الحوكمة وبرامج الحماية لمؤسسات وجهات البنى التحتية للمعلومات الحيوية، وبما يشتمل على تحديد هذه المؤسسات، والمتطلبات الأساسية لها، وآليات الإشراف على المتطلبات وإنفاذها فيما يتعلق بحماية البنى التحتية للمعلومات الحيوية.

1.2 النطاق ومدى قابلية التطبيق

البنية التحتية للمعلومات الحيوية

تعرّف بأنها "أنظمة المعلومات، والأصول الرقمية، والشبكات، والخدمات، والتركيبات المترابطة التي تُستخدم لتقديم ودعم الخدمات الوطنية الحيوية في دولة الإمارات العربية المتحدة".

أما الخدمات الوطنية الحيوية، فهي: الخدمات المادية أو الافتراضية، التي تُعد غاية في الأهمية لدولة الإمارات العربية، والتي وإن تعرض أي منها للتعطيل أو الإتلاف فإن هذا الأمر سيكون له أثر جسيم وملموس على الأمن الوطني، والأمن أو الصحة العامة، والقدرة على الأداء الفعّال للوظائف الحكومية، أو أي مما سبق مجتمعة أم منفردة.

وتتضمن مؤسسات البنى التحتية للمعلومات الحيوية جميع الجهات المالكة والمسؤولة ضمن القطاعين العام والخاص، وأي جهة أخرى تؤدي دوراً في تأمين الخدمات الحيوية وما تتضمن جميع فئات التكنولوجيا، وبما يشتمل على تكنولوجيا المعلومات ، وأنظمة التحكّم الصناعي، والنظم السيبرانية المادية، وبشكل أوسع جميع الأجهزة المتصلة بما فيها إنترنت الأشياء، وإنترنت الأشياء الصناعية.

حدّدت دولة الإمارات القطاعات التالية على أنها قطاعات "حيوية" عند الأخذ بعين الاعتبار مستوى الأثر الذي تسببه على الأمن الوطني، والأمن الاقتصادي، والصحة والسلامة العامة، والاستقرار السياسي، وجميع التبعيات المتبادلة ذات الصلة.

وتُعد هذه السياسة بأنها قابلة للتطبيق على المؤسسات والجهات المعنية بالبنى التحتية للمعلومات الحيوية، والجهات المنظّمة والجهات المعنية ضمن القطاعات ذات العلاقة، وجميع الجهات المعنية المشاركة ضمن القطاعات والقطاعات الفرعية التالية، بالإضافة إلى أي قطاع آخر يحدّده مجلس الأمن السيبراني.

1.2 النطاق ومدى قابلية التطبيق

القطاع الحيوي	القطاع الفرعي	اسم المجموعة (بحسب ما نص عليه الإطار الوطني لحوكمة الأمن السيبراني)	نوع الجهة
الطاقة	النفط	المجموعة أ	• الهيئات • الجهات المشغلة لعمليات استكشاف النفط الخام، وإنتاجه، وجميع المنشآت المعنية بمعالجته وتصفيته، وتخزينه، وأنابيب نقله • سلسلة التوريد والمرافق اللوجستية • الجهات المركزية المالكة لأسهم النفط والمسؤولة عن تجارته في الأسواق • البنية التحتية
	الغاز	المجموعة أ	• الهيئات • الجهات المشغلة لعمليات استكشاف الغاز المسال، وإنتاجه، وجميع المنشآت المعنية بمعالجته وتصفيته، وتخزينه، وأنابيب نقله • سلسلة التوريد والمرافق اللوجستية • البنية التحتية
	الطاقة النووية	المجموعة أ	• الهيئات • الجهات المشغّلة لمحطات التخصيب النووية ومنشآت الوقود المستهلك • سلسلة التوريد والمرافق اللوجستية • البنية التحتية
النقل	النقل الجوي	المجموعة أ	• الهيئات • الناقلون الجويون • سلطات النقل الجوي • إدارة الحركة الجوية • شركات إدارة المطارات • الجهات المشغّلة لعملية التحكّم في إدارة الحركة الذين يقدّمون خدمات مراقبة الحركة الجوية
	السكك الحديدية	المجموعة ب	• الهيئات • الجهات المشغّلة • إدارة السكك الحديدية، بما يتضمن الجهات المشغّلة للمنشآت الخدمية • البنية التحتية
	النقل البحري	المجموعة ب	• الهيئات • الجهات المشغّلة للسفن • السلطات والجهات المشغّلة للموانئ • الجهات المسؤولة عن إدارة الموانئ، والمؤسسات المشغّلة للأعمال والمعدات المتواجدة داخل الموانئ • الجهات المشغّلة لخدمات حركة مرور السفن • البنية التحتية
	الطرق	المجموعة ب	• الهيئات • إدارة حركة المرور • الجهات المشغّلة لأنظمة النقل الذكية • البنية التحتية

1.2 النطاق ومدى قابلية التطبيق

القطاع الحيوي	القطاع الفرعي	اسم المجموعة (بحسب ما نص عليه الإطار الوطني لحوكمة الأمن السيبراني)	نوع الجهة
القطاع المالي	السلطات والجهات المنظّمة للقطاع المالي	المجموعة أ	• المؤسسات المرخصة والخاضعة لتنظيم مصرف الإمارات العربية المتحدة المركزي • مؤسسات الإقراض • التأمين
	مقدّمو الخدمات المالية	المجموعة أ	• مقدّم خدمات بوابات الدفع • مقدّمو خدمات أجهزة الصرافة الآلية
الصحة	السلطات والجهات المنظّمة للقطاع الصحي	المجموعة ب	• مقدّمو الخدمات الصحية • خدمات بيانات الرعاية الصحية • الجهات المصنّعة وشركات توزيع الأجهزة الطبية • الجهات المصنّعة وشركات توزيع الأدوية • مختبرات البحث والتطوير
المياه والكهرباء	الكهرباء	المجموعة ب	• مؤسسات توريد الكهرباء (الجهات المتعهدة) التي تؤدي وظيفة "تزويد الطاقة" • الجهات المشغّلة لمنشآت التوليد • الجهات المشغّلة لأنظمة النقل • الجهات المشغّلة لأنظمة التوزيع • الجهات المُختارة المشغّلة لأسواق الكهرباء • الجهات المشاركة في سوق الكهرباء • تبريد المناطق مع تعزيز استخدام الطاقة من المصادر المتجددة
	البنية التحتية الحيوية للمياه	المجموعة ب	• أنابيب التوزيع للاستهلاك الصناعي والبشري • محطات الضخ • مصانع التحلية • مصانع المعالجة
	السلطات المسؤولية والجهات المقدّمة للخدمات	المجموعة ب	• شركات وهيئات توزيع الكهرباء والماء
	مياه الصرف الصحي	المجموعة ب	• محطات معالجة المياه العادمة • مرافق معالجة مياه الصرف الصحي الناتجة عن الاستعمالات الصناعية • شبكة أنابيب الصرف الصحي

1.2 النطاق ومدى قابلية التطبيق

القطاع الحيوي	القطاع الفرعي	اسم المجموعة (بحسب ما نص عليه الإطار الوطني لحوكمة الأمن السيبراني)	نوع الجهة
البنية التحتية الرقمية		المجموعة أ	• مقدّمو خدمات الاتصالات السلكية واللاسلكية والإنترنت • مقدّمو البنى التحتية لنظام أسماء النطاقات • مقدّمو خدمات الحوسبة السحابية • مقدّمو خدمات مراكز البيانات • الجهات المصنّعة وشركات توزيع معدات الاتصالات وتكنولوجيا المعلومات وأنظمة التحكّم الصناعي وإنترنت الأشياء • مقدّمو نقاط تبادل الإنترنت • أنظمة الكوابل البحرية • مقدّمو خدمات الاتصالات الإلكترونية الذين يوفّرون خدماتهم للاستخدام العام
الخدمات الحكومية	الوزارات والهيئات الاتحادية	المجموعة أ	• جميع السلطات والأجهزة الاتحادية، وجميع الوزارات
	على مستوى حكومة دولة الإمارات العربية المتحدة	المجموعة ب	• جميع الجهات الحكومية المحلية القائمة داخل كل إمارة
التعليم		المجموعة أ	• الجهات من القطاعين العام والخاص • مقدّمو الخدمات الرقمية للتعليم عن بُعد
الفضاء		المجموعة أ	• جميع الجهات المختصة
الصناعات الغذائية		المجموعة أ	• إنتاج وتوزيع الغذاء

1.2 النطاق ومدى قابلية التطبيق

المجموعة أ

تندرج الجهات التي تنتمي إلى هذه المجموعة تحت القطاعات التالية، والتي تعمل في الغالب ضمن سياق قطاعي في دولة الإمارات العربية المتحدة:

- البنية التحتية الرقمية
- الخدمات المالية
- النقل الجوي
- الطاقة (النووية)
- الطاقة - قطاع النفط والغاز
- الفضاء
- الأغذية
- التعليم

وتُصنّف الجهات التابعة لهذه القطاعات إلى مجموعتين، وهما: الجهات المعنية بالبنى التحتية للمعلومات الحيوية، والجهات غير المعنية بالبنى التحتية للمعلومات الحيوية، حيث تتولى الجهات القائدة ضمن القطاع المسؤولية عن تصنيف هذه الجهات.

ويجب أن تمتثل هذه الجهات للقوانين واللوائح المفروضة في الدولة، كما يجب أن تتبنى نهجاً فعّالاً لتحديد المخاطر وتنفيذ متطلبات الأمن السيبراني بما يتماشى مع السياسات والمعايير والإرشادات الوطنية، بما يشمل أي متطلبات خاصة بالإمارة والقطاع، وإعداد التقارير المتعلقة بالامتثال دورياً وحسب الحاجة.

المجموعة ب

وتندرج الجهات التي تنتمي إلى هذه المجموعة تحت القطاعات التالية، والتي تعمل في الغالب ضمن كل إمارة:

- النقل - السكك الحديدية والطرق والنقل البحري
- المياه والكهرباء
- الرعاية الصحية

وتُصنّف الجهات التابعة لهذه القطاعات إلى مجموعتين، وهما: الجهات المعنية بالبنى التحتية للمعلومات الحيوية، والجهات غير المعنية بالبنى التحتية للمعلومات الحيوية، حيث تتولى الجهات القائدة ضمن القطاع المسؤولية عن تصنيف هذه الجهات.

ويجب أن تمتثل هذه الجهات للقوانين واللوائح المفروضة في الدولة، كما يجب أن تتبنى نهجاً فعّالاً لتحديد المخاطر وتنفيذ متطلبات الأمن السيبراني بما يتماشى مع السياسات والمعايير والإرشادات الوطنية، بما يشمل أي متطلبات خاصة بالإمارة والقطاع، وإعداد التقارير المتعلقة بالامتثال دورياً وحسب الحاجة.

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 هذه الخطوات التحسين المستمر لقدرات الأمن السيبراني في دولة الإمارات العربية المتحدة وبما يضمن إيجاد المتطلبات لتأمين وحماية البنى التحتية للمعلومات الحيوية.

فهم مستوى التعقيد، وازدياد مستوى التبعيات، وفهم القوانين واللوائح المعمول بها، والدوافع وراء تحديد أولويات الخدمات الحيوية، والتغيير في مشهد التهديدات، والتحديات التي تواجه تنفيذ نهج موحّد لحماية البنى التحتية للمعلومات الحيوية.

تقييم المخاطر التي تتعرض لها الخدمات والعمليات الحيوية، والأصول الرقمية، وتحديد الأثر النسبي، وتقييم الوضع الحالي للضوابط الأمنية المعمول بها، وتحديد مخاطر وقوع الخروقات أو الفشل المحتمل، ووضع خطط للتخفيف من حدة المخاطر.

تطبيق الضوابط الأمنية المحدّدة وأفضل الممارسات المعتمدة داخل الدولة ضمن القطاعات الحيوية من خلال التعاون المستمر وتبادل المعلومات.

مراقبة ومراجعة أداء وفاعلية الضوابط الأمنية المطبّقة بغرض التحسين المستمر.

التعاون مع القطاعات الحيوية الأخرى، ومع المؤسسات الوطنية، والجهات المحلية والإقليمية والعالمية العاملة في هذا المجال، والتعاون مع الجهات من القطاعين العام والخاص، لتبادل المعلومات واعتماد وتبني أفضل الممارسات.

1.4 مبادئ حماية البنية التحتية للمعلومات الحيوية

وُضعت المبادئ التالية المتعلقة بحماية البنى التحتية للمعلومات الحيوية كعناصر وظيفية لحماية البنى التحتية للمعلومات الحيوية في الدولة، كما أنها استُخدمت لوضع سياسة حماية البنى التحتية للمعلومات الحيوية.

تعزيز المرونة السيبرانية على المستوى الوطني

إيجاد مفاهيم الموثوقية وتكرار الوظائف وقدرات الاستجابة والتعافي والحفاظ عليها في الجهات المعنية بالبنية التحتية للمعلومات الحيوية، وذلك بهدف تحفيز المرونة السيبرانية على المستوى الوطني

الحكومة المتركزة على القطاع

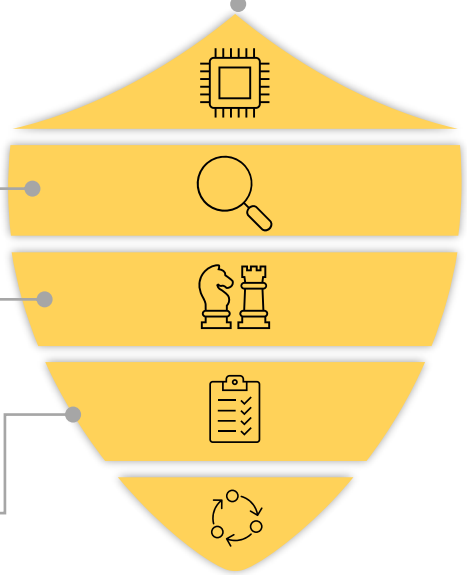
أُسّست هياكل الحوكمة ضمن كل قطاع بهدف بناء القدرات اللازمة لتلبية الاحتياجات على مستوى القطاعات؛ وهو ما يهدف إلى تمكين عمليات التدخل الهادفة، وتعزيز الابتكارات والقدرة التنافسية الداخلية في القطاعات المحدّدة.

تحديد الأولويات اعتماداً على مستوى المخاطر

تبنّي النهج المبني على تحديد الأولويات اعتماداً على مستوى المخاطر، وذلك بهدف تحديد الضوابط والإجراءات الأمنية، وإعداد البرنامج الوطني للبنية التحتية للمعلومات الحيوية.

إعداد المعايير وأفضل الممارسات المتبعة

يُستفاد من أفضل الممارسات العالمية لتوفير الأمان وتعزيز كفاءات الامتثال، في حين وُضع الحد الأدنى من المتطلبات إلزامياً للبنى التحتية للمعلومات الحيوية الخاضعة للمراقبة باستمرار.



تشجيع التعاون والشراكات

تحتاج حماية البنية التحتية للمعلومات الحيوية بفاعلية إلى التواصل والتنسيق والتعاون بين كافة الجهات المعنية على المستويين الوطني والدولي، وذلك بهدف خلق ثقافة الثقة وتعزيز مستويات الأمن الوطني.

1.5 الموافقة على الاستثناءات

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

ستُراجع الاستثناءات على أساس كل حالة على حدة، ولا تُضمن الموافقة عليها.

القسم 2

سياسات حماية البنية التحتية للمعلومات الحيوية

يوضّح القسم التالي نطاقات السياسة الرئيسية منها والفرعية على حماية البنية التحتية للمعلومات الحيوية، وتركّز النطاقات الفرعية للسياسة تركيزاً أكبر على أهدافها وبياناتها:

2.1 الحوكمة لبرنامج حماية البنى التحتية للمعلومات الحيوية

2.1.1 الحوكمة على المستوى الوطني

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

تقديم الإشراف والتوجيه لمختلف القطاعات والقطاعات الفرعية والجهات المشغّلة والجهات المعنية ببنية المعلومات الحيوية

بيانات السياسة

2.1.1.1 يقود مجلس الأمن السيبراني أنشطة تنفيذ برنامج حماية البنية التحتية للمعلومات الحيوية في كافة القطاعات (الرئيسية والفرعية) والجهات المشغّلة والجهات العاملة ضمن إطار البنية التحتية للمعلومات الحيوية، فضلاً عن تطوير نظام خاص للمراقبة ورفع التقارير بما يتماشى مع مختلف الوزارات والهيئات الاتحادية والجهات المسؤولة عن القطاعات المعنية والجهات المسؤولة عن كل إمارة.

2.1.1.2 تُحدّد الأدوار والمسؤوليات الرئيسية المنوطة بالجهات المسؤولة عن القطاعات المعنية وكل إمارة من خلال الإطار الوطني لحوكمة الأمن السيبراني.

2.1.1.3 تُدار كل جهة موجودة ضمن القطاعات الرئيسية بحسب نموذج الحوكمة المنصوص عليه في الإطار الوطني لحوكمة الأمن السيبراني.

2.1 الحوكمة لبرنامج حماية البنى التحتية للمعلومات الحيوية

2.1.2 الحوكمة على مستوى الإمارة

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

تقديم الدعم للجهات المعنية بالبنية التحتية للمعلومات الحيوية ضمن المجموعة أ، والمساعدة في مراقبة عملية تنفيذ برنامج حماية البنية التحتية للمعلومات الحيوية.

بيانات السياسة

2.1.2.1 تقدّم الجهة المسؤولة على مستوى الإمارة الدعم للجهات المعنية بالبنى التحتية للمعلومات الحيوية ضمن المجموعة أ، وتساعد في تطبيق المعايير والسياسات واللوائح الوطنية في كل الإمارة، بالإضافة إلى المعايير واللوائح وقوانين الأمان والخصوصية التي تتبناها كل إمارة.

2.1.2.2 تراقب كل جهة مسؤولة على مستوى الإمارة تنفيذ برنامج حماية البنية التحتية للمعلومات الحيوية للجهات المعنية بالبنى التحتية للمعلومات الحيوية ضمن المجموعة أ، وترفع تقارير الامتثال إلى الجهات الوطنية حسب الحاجة.

2.1.2.3 يجب المحافظة على لائحة الجهات المعنية بالبنى التحتية للمعلومات الحيوية وإيصالها إلى مجلس الأمن السيبراني والهيئات ذات العلاقة، كما يجب مراجعة اللائحة وتحديثها بانتظام.

2.1 الحوكمة لبرنامج حماية البنى التحتية للمعلومات الحيوية

2.1.3 الحوكمة على مستوى القطاعات

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

تقديم الإرشاد والتوجيه للجهات المشغّلة والجهات المعنية بالبنية التحتية للمعلومات الحيوية ضمن القطاع والاضطلاع بمسؤولية تنفيذ برنامج حماية البنية التحتية للمعلومات الحيوية ضمن هذا القطاع.

بيانات السياسة

2.1.3.1 تقود الجهة المسؤولة عن القطاعات المعنية مهام تنفيذ برنامج حماية البنية التحتية للمعلومات الحيوية لكافة الجهات في المجموعة أ، بالإضافة إلى المراقبة المستمرة للتنفيذ ورفع التقارير الدورية إلى الجهات الوطنية ذات الصلة.

2.1.3.2 يجري اختيار الجهات المنظّمة للقطاع أو الجهة المسؤولة عن القطاع بهدف ضمان تنفيذ الأنشطة في القطاع بما يتماشى مع الأدوار والمسؤوليات الواردة في الإطار الوطني لحوكمة الأمن السيبراني.

2.1.3.3 يجب المحافظة على لائحة الجهات المعنية بالبنى التحتية للمعلومات الحيوية وإيصالها إلى مجلس الأمن السيبراني والجهات المسؤولة عن كل إمارة والجهات المسؤولة عن القطاعات المعنية الاخرى عند الحاجة، كما يجب مراجعة اللائحة وتحديثها بانتظام.

2.1 الحوكمة لبرنامج حماية البنى التحتية للمعلومات الحيوية

2.1.4 الحوكمة على مستوى الجهة المشغّلة/ الجهة المعنية بالبنى التحتية للمعلومات الحيوية

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

ضمان فهم الجهات المشغّلة والجهات المعنية بالبنى التحتية للمعلومات الحيوية لأدوارهم ومسؤولياتهم تجاه تهيئة بنية تحتية آمنة للمعلومات.

بيانات السياسة

2.1.4.1 يتعيّن على كافة الجهات المشغّلة والجهات المعنية بالبنى التحتية للمعلومات الحيوية المشمولة تحت هذه السياسة إنشاء قسم خاص للإدارة الأمنية وتعيين طاقم عمل متخصص لإدارة وتلبية متطلبات الجهة من ناحية الأمن السيبراني.

2.1.4.2 يتولى قسم الإدارة الأمنية المهام التالية:

- تنفيذ التقييمات السنوية للمخاطر بما يتماشى مع المتطلبات المنصوص عليها في الإطار الوطني لإدارة المخاطر السيبرانية أو ما يعادلها من أفضل الممارسات الدولية، وذلك إما بأنفسها أو من خلال الشركات المقدّمة لهذه الخدمات، ويتعيّن على القسم أيضاً تقديم نتائج التقييمات ومقاييس التحسين إلى بوابة أمن الإشارات المسؤولة عن أمن البنية التحتية للمعلومات الحيوية.
- وضع خطط الأمن السيبراني وتصميمها وتحسينها باستمرار ضمن الجهة.
- بناء قدرات الدخول والمراقبة ضمن الجهة بطريقة تتكامل مع مراكز العمليات الأمنية على مستوى القطاع والمستوى الوطني.
- الحرص على عزل شبكة التكنولوجيا التشغيلية وأنظمة التحكّم الصناعي (حيثما ينطبق)
- وضع خطط الطوارئ وتنفيذ التدريبات التي تحاكي أرض الواقع وإدارة حوادث الأمن السيبراني بما يتماشى مع متطلبات الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث
- عقد البرامج التعليمية والتدريب الفني وتقييم المهارات في مجال الأمن السيبراني.
- مراقبة المنتجات والخدمات المقدّمة من الجهات الخارجية من خلال إعطاء الأولوية لشراء المنتجات والخدمات الآمنة والموثوقة، وتوقيع اتفاقيات الحفاظ على السرية، وإجراء المراجعات المستقلة دورياً وحسب الحاجة.
- التنسيق مع الهيئة التنظيمية المختصة وإبلاغها (1) بأي تغيير رئيسي حصل في البنية التحتية للمعلومات الحيوية بصورة قد تؤثر على تصنيف الجهة ضمن إحدى الجهات المشغّلة للبنى التحتية للمعلومات الحيوية، (2) الإبلاغ عن عمليات الدمج أو الانقسام أو التفكك أو أي تغيير رئيسي آخر قد يحصل على الهيكل التنظيمي للجهة، (3) الإبلاغ عن أي قضايا أو تهديدات رئيسية على الأمن السيبراني.

2.1 الحوكمة لبرنامج حماية البنى التحتية للمعلومات الحيوية

2.1.5 إدارة سلسلة التوريد

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

تقليص المخاطر التي قد تترتب عن استخدام البرمجيات التابعة لجهات خارجية، وتأمين البيانات التي يُمكن الوصول إليها من قبل موظفي الجهات الخارجية وضمان عدم الإفصاح عنها أو العبث بها.

بيانات السياسة

2.1.5.1 تتحمل كافة الجهات المعنية بالبنى التحتية للمعلومات الحيوية، التي تعتمد على المنتجات والخدمات التابعة للجهات الخارجية، مسؤولية حماية الخدمات الحيوية وضمان تلبية المتطلبات الأمنية ذات الصلة بصرف النظر عما إذا كانت الخدمات مقدّمة من الجهة المعنية بالبنى التحتية للمعلومات الحيوية أو جهة خارجية.

2.1.5.2 يتعيّن على كافة الجهات المشغّلة والجهات المعنية بالبنى التحتية للمعلومات الحيوية تطوير استراتيجية لتأمين سلسلة التوريد من خلال اتباع مبادئ إدارة المخاطر والدفاع السيبراني.

2.1.5.3 يجب على كافة الجهات المشغّلة والجهات المعنية بالبنى التحتية للمعلومات الحيوية مراعاة الجوانب التالية:

- التعامل مع المورّدين المعتمدين.
- إجراء عمليات التحقّق اللازمة لطاقم العمل الرئيسي التابع للجهات الخارجية.
- فرض حد أدنى من متطلبات الأمن السيبراني ليلتزم بها المورّدون.
- تقييد مستوى التصريحات وإمكانية الدخول والبرامج المسموحة للمورّدين.
- التحقّق من كافة عمليات نقل البيانات ومراقبتها.
- إجراء التقييمات الأمنية (بما يتضمن التقييمات الأمنية الفنية) بما يتماشى مع القوانين ذات الصلة والسياسات الوطنية والمتطلبات على مستوى الإمارة أو القطاع.
- توقيع اتفاقيات السرية أو الأمن بصورة توضّح متطلبات الدعم الفني والجوانب الفنية ومتطلبات السرية.

2.1 الحوكمة لبرنامج حماية البنى التحتية للمعلومات الحيوية

2.1.6 متطلبات أمن البيانات والخصوصية

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

الحرص على حماية البيانات بفاعلية وضمن إطار القانون باتباع الإجراءات الضرورية، والحفاظ على المستوى الأمني المطلوب.

بيانات السياسة

2.1.6.1 يتعيّن على الجهات المشغّلة والجهات المعنية بالبنى التحتية للمعلومات الحيوية تحديد واتباع الأنظمة والقوانين الخاصة بخصوصية البيانات على الصعيد الوطني وعلى مستوى الإمارة.

2.1.6.2 يتعيّن على الجهات المشغّلة والجهات المعنية بالبنى التحتية للمعلومات الحيوية تصنيف البيانات وحمايتها بناءً على أهميتها ومدى تأثيرها على التنمية الاقتصادية والأمن الوطني والمصلحة العامة والحقوق الشرعية ومصالح الأفراد والجهات على حد سواء.

2.2 إعداد سجل المخاطر

2.2.1 تحديد الخدمات الحيوية وترتيبها حسب الأولوية

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

ضمان قيام الجهات بتحديد الخدمات الحيوية باتباع منهج منتظم.

بيانات السياسة

2.2.1.1 يتعيّن على الجهات المعنية بالبنى التحتية للمعلومات الحيوية اتباع منهج منظم لتحديد الخدمات الحيوية وترتيبها حسب الأولوية، وذلك بناءً على أفضل الممارسات المحدّدة في الإطار الوطني لإدارة المخاطر السيبرانية، الأمر الذي يسمح باختيار هذه الخدمات بالاستناد إلى معايير قابلة للقياس الكمي بدلاً من اتباع المعايير غير الموضوعية.

2.2.1.2 قد تراعي عملية تحديد الخدمات الحيوية الجوانب التالية إلى جانب الإرشادات الواردة في الإطار الوطني لإدارة المخاطر السيبرانية:

- المعايير الخاصة بالقطاع: قد يشمل ذلك حصة السوق، أو الخدمات ذات نقطة التعطل المنفردة، أو الاتصال عبر الحدود، أو توريد الخدمات إلى الجهات الحكومية أو القطاع أو العامة، وغير ذلك.
- التبعية: يشمل ذلك مستوى التبعيات ضمن قطاعات البنية التحتية الحيوية الأخرى ومنتجاتها أو خدماتها، أو التبعيات ضمن سلسلة التوريد، أو التبعيات التي يترتب عليها حدوث تعطّل بشكل متكرر، أو التبعيات في أوقات الطوارئ أو حالات التعافي.
- نطاق الأثر: قد يتضمن ذلك التأثير ضمن الجهة نفسها أو على منطقة كبيرة أو ضمن قطاعات متعددة (بشكل نسبي)، أو على المستوى الوطني أو على مستوى القطاع بأكمله، أو على المستوى الدولي أو على مستوى العديد من القطاعات (بشكل كامل)، فضلاً عن نسبة المتأثرين من العامة الناس أو نسبة الأفراد المتأثرين ضمن المنطقة المتأثرة.

2.2 إعداد سجل المخاطر

2.2.2 إجراء تقييم المخاطر

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

الحرص على قيام كافة الجهات بإجراء تقييم المخاطر بانتظام بهدف تحديد المخاطر التي قد تؤثر على الخدمات الحيوية والبنية التحتية للمعلومات.

بيانات السياسة

2.2.2.1 يتعيّن على الجهات تحديد العناصر الأساسية للخدمات؛ بمعنى أن غياب هذه العناصر سيؤدي إلى فقدان الخدمة الحيوية. وتشمل هذه العناصر أنظمة المعلومات والأصول الرقمية والشبكات وأنظمة وشبكات التحكّم الصناعية وعناصر سلسلة التوريد والأجهزة والمعدات والمرافق وطواقم العمل التي تدعم الخدمات الحيوية.

2.2.2.2 يتعيّن على الجهات إجراء تقييم سنوي للمخاطر الأمنية بحيث يركّز على المكونات المُحدّدة في البنية التحتية للمعلومات الحيوية، وذلك من أجل الحماية من الفشل المتعلق بمستوى التكامل ومدى التوفّر والسرية.

2.2.2.3 يتعيّن على الجهات تحليل أثر التهديدات ومستوى تأثيرها على مكونات البنية التحتية للمعلومات الحيوية، وذلك من أجل تحديد المخاطر الأساسية والتعامل معها. ويجب أيضاً تحديد الضوابط الحالية من أجل استخراج المخاطر المتبقية بحسب المعايير المتبعة في الإطار الوطني لإدارة المخاطر السيبرانية.

2.2.2.4 يتعيّن على الجهات وضع إطار عمل لتنظيم أنشطة التواصل ورفع التقارير، وسيساهم ذلك في مشاركة نتائج تقييمات المخاطر مع الهيئات التنظيمية والسلطات على مستوى القطاع أو الإمارة.

2.2 إعداد سجل المخاطر

2.2.3 إعداد سجل المخاطر للقطاع وعلى المستوى الوطني

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

إعداد سجل المخاطر المخصّص للقطاع وعلى المستوى الوطني ووضع خطط التحسين ذات الصلة وتعزيز إجراءات الحماية ضد المخاطر المحدّدة.

بيانات السياسة

2.2.3.1 يتعيّن على كافة الجهات العاملة ضمن القطاع التواصل مع الجهات المسؤولة عن القطاع معنية أو الجهات المسؤولة على مستوى الإمارة حول المخاطر الرئيسية المحدّدة، وتقديم الدعم في إعداد سجل المخاطر على مستوى القطاعات ووضع خطط التحسين المبنية على هذا السجل.

2.2.3.2 ومن جانبه، يتعاون مجلس الأمن السيبراني مع الجهات المسؤولة عن كل قطاع وإمارة لمناقشة هذه المخاطر الرئيسية المُحدّدة ضمن القطاع ودراسة التهديدات المشتركة والمخاطر المشتركة بين القطاعات بهدف إعداد سجل وطني للمخاطر ووضع خطط التحسين بناءً عليه.

2.3 برنامج حماية البنية التحتية للمعلومات الحيوية

2.3.1 اتباع التوجهات الوطنية بشأن الأمن السيبراني

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

تنفيذ المتطلبات الوطنية للأمن السيبراني واتباعها

بيانات السياسة

2.3.1.1 يقوم مجلس الأمن السيبراني، بالتعاون مع الجهات المسؤولة عن كل قطاع وإمارة، بإيضاح السياسات والمعايير الضرورية للأمن السيبراني وإرساله إلى القطاعات والجهات المعنية بالبنى التحتية للمعلومات الحيوية. وسيساهم ذلك في وضع خطة حماية البنية التحتية للمعلومات الحيوية ضمن القطاع.

2.3.1.2 يقوم مجلس الأمن السيبراني، بالتعاون مع الجهات المسؤولة عن كل قطاع وإمارة، بإيضاح الخطة الوطنية المتبعة لبرنامج حماية البنية التحتية للمعلومات الحيوية، ويشمل ذلك أي اعتبارات متعلقة بالقطاعات.

2.3.1.3 يتعيّن على كافة الجهات المعنية بالبنى التحتية للمعلومات الحيوية تنفيذ سياسات الأمن السيبراني ومعاييره وأسسه وخططه بحسب الحاجة وبحسب توجهات مجلس الامن السيبراني و/ أو الجهات المسؤولة عن كل قطاع أو إمارة.

2.3.1.4 يتعيّن على الجهات المعنية بالبنى التحتية للمعلومات الحيوية تلبية متطلبات الأمن السيبراني المخصّصة للقطاع أو الصناعة أو المجال، وذلك لحماية البنية التحتية لمعلوماتها والحرص على توفّرها وسريتها.

2.3 برنامج حماية البنية التحتية للمعلومات الحيوية

2.3.2 التعامل مع التبعيات الرقمية المتبادلة

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	الضمان

هدف السياسة

التعامل مع المخاطر المنهجية وتقليص الأثر السلبي المترتب على التبعيات الرقمية المتبادلة والعلاقات بين البنى التحتية للمعلومات الحيوية، وتعزيز مستوى المرونة والأداء لإجراءات تقليص المخاطر.

بيانات السياسة

2.3.2.1 يجب على الجهات المعنية بالبنى التحتية للمعلومات الحيوية فهم مستوى التبعيات والتبعيات المتبادلة ضمن القطاعات أو الجهات الحيوية الأخرى من خلال إجراء تقييمات للمراحل الأولية والنهائية، بالإضافة إلى تحديد مستوى التبعيات المتبادلة الداخلية للجوانب التالية:

- المنتجات أو الخدمات المقدّمة إلى الجهة من قبل جهة خارجية تُعد مهمة لدعم العمليات والوظائف
- مستوى التبعيات المتبادلة أثناء العمليات الاعتيادية وأثناء فترات الاستجابة للأزمات
- التبعيات الخارجية
- التبعيات المتبادلة بين الجهات العامة والخاصة

2.3.2.2 يستعان لعملية تقييم نوع الفشل أو العطل (سبب مشترك أو انتشار أو تسلسل) لتوجيه إجراءات تقليص الأثر.

2.3.2.3 ستساهم حماية السرية والسلامة ومستوى التوفّر للبنى التحتية للمعلومات الحيوية في التعامل مع مسألة دمج أجهزة إنترنت الأشياء في البنية التحتية للمعلومات الحيوية، وتحقيق التوافق بين تكنولوجيا المعلومات والتكنولوجيا التشغيلية.

2.3.2.4 يتعيّن على الجهات المعنية بالبنى التحتية للمعلومات الحيوية وضع خطة حماية البنية التحتية للمعلومات الحيوية بناءً على الاعتبارات أعلاه.

2.3 برنامج حماية البنية التحتية للمعلومات الحيوية

2.3.3 تبادل المعلومات والتنسيق

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

تعزيز ثقافة الثقة بين الجهات المعنية بالبنية التحتية للمعلومات الحيوية، بما يتضمن تبادل المعلومات الحساسة وتحديد المنهج المتبع للتعاون الدولي.

بيانات السياسة

2.3.3.1 يتعيّن على كافة الجهات المعنية بالبنى التحتية للمعلومات الحيوية تنفيذ الإجراءات المطلوبة في سياسة تبادل المعلومات، بما يتضمن إجراءات تحديد نوع المعلومات الواجب مشاركتها وشروط تبادل المعلومات مع الجهات المعنية.

2.3.3.2 وفقاً لما يرد في النموذج الوطني لحوكمة الأمن السيبراني، يتعيّن على كافة الجهات المعنية بالبنى التحتية للمعلومات الحيوية تبادل المعلومات المتعلقة بالمخاطر والثغرات الأمنية مع الجهات المنظّمة في القطاع أو الجهة المسؤولة في كل إمارة وضمن مجموعات تبادل المعلومات، الأمر الذي يساهم في تهيئة بيئة تعاونية وعالية الفاعلية.

2.3.3.3 يساهم مجلس الأمن السيبراني في تطوير القدرات على المستوى الوطني من أجل تحديد التهديدات والثغرات ونشر المعلومات الفورية والهامة إلى القطاعات الحيوية والجهات المعنية بالبنى التحتية للمعلومات الحيوية.

2.3.3.4 يتعيّن على الجهات المعنية بالبنى التحتية للمعلومات الحيوية تبادل المعلومات المتعلقة بالتهديدات السيبرانية، ويشمل ذلك مؤشرات الاختراق، الأساليب والتكتيكات والإجراءات المتبعة لتحديد الهجمات وردعها، مع المراكز الوطنية المختصة بالتحليل الذكي للمخاطر.

2.3.3.5 يوفّر مجلس الأمن السيبراني التوجيهات حول عمليات الإفصاح المتعلقة بحماية البنية التحتية للمعلومات الحيوية، بما يتضمن المعلومات السرية أو المملوكة، والضمانات المطلوبة للسرية والأمن الرقمي، وذلك بهدف إقامة علاقات موثوق بها وتعزيز التعاون بين القطاعين العام والخاص.

2.3.3.6 يساهم مجلس الأمن السيبراني في أنشطة التعاون الدولي الرامية إلى تأمين البنية التحتية للمعلومات الحيوية، بما يشمل تطوير أنظمة الإنذار في حالات الطوارئ، ومشاركة وتحليل الثغرات ذات الصلة، والتهديدات، ومعلومات الحوادث، والتنسيق لإجراء التحريات حول الهجمات السيبرانية على البنى التحتية، بما يتماشى مع القوانين الداخلية.

2.3 برنامج حماية البنية التحتية للمعلومات الحيوية

2.3.4 تعزيز المرونة على المستوى الوطني

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

تعزيز الجاهزية الوطنية وبناء قدرات الاستجابة والتعافي من حوادث الأمن السيبراني

بيانات السياسة

2.3.4.1 يتعيّن على الجهات المعنية بالبنى التحتية للمعلومات الحيوية الحرص على تحديد وتنفيذ كافة الجوانب الضرورية لبناء القدرات التي تساهم في منع تعطل البنى التحتية للمعلومات الحيوية واستمرارية خدماتها، بما يشمل الضوابط الفنية والتقنية، بالاستناد إلى تقييم المخاطر التي تجريه الجهات.

2.3.4.2 يتعيّن على الجهات المعنية بالبنى التحتية للمعلومات الحيوية اتباع المعايير الأساسية المعتمدة لدى المركز الوطني للعمليات الأمنية من أجل ضمان فهم كافة مستويات الأثر الناجم عن الحوادث والحفاظ بأقل تقدير على اتباع الحد الأدنى من المعايير المعتمدة لدى مركز العمليات الأمنية، وتحقيق القدرات المستهدفة.

2.3.4.3 يقوم مجلس الأمن السيبراني بتطوير شبكات لإدارة الحوادث وأنشطة التواصل أثناء الأزمات، بالإضافة إلى تحديد المتطلبات للجهات المعنية بالبنى التحتية للمعلومات الحيوية ضمن إطار الاستجابة للحوادث السيبرانية.

2.3.4.4 يتعيّن على الجهات المعنية بالبنى التحتية للمعلومات الحيوية الاستجابة للحوادث السيبرانية المهمة بانتظام كما هو وارد في خطة الاستجابة للحوادث السيبرانية، وذلك بهدف تقليص أثر ونطاق هذه الحوادث.

2.3.4.5 يتعيّن على الجهات المعنية بالبنى التحتية للمعلومات الحيوية اتباع المعايير المشتركة لمواجهة حوادث الأمن الرقمي ضمن القطاع.

2.3.4.6 يتعيّن على الجهات المعنية بالبنى التحتية للمعلومات الحيوية إجراء التدريبات السيبرانية التي تحاكي الواقع لاختبار مدى مرونة الأنظمة والخدمات الحيوية، بالإضافة إلى المشاركة في الاختبارات القائمة على المستوى الوطني أو على مستوى القطاعات من أجل التحقّق من مستوى المرونة السيبرانية.

2.4 ضمان برنامج حماية البنى التحتية للمعلومات الحيوية

2.4.1 آلية التطبيق

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

بيان آلية تنفيذ مسؤوليات ومهام برنامج حماية البنية التحتية للمعلومات الحيوية.

بيانات السياسة

2.4.1.1 يعمل مجلس الأمن السيبراني على إنفاذ السياسات والمعايير الإلزامية وتنفيذ عمليات التفتيش والمراجعة الدورية ومراقبة مستوى الامتثال للتحقّق من أمن البنى التحتية للمعلومات الحيوية.

2.4.1.2 يحدّد مجلس الأمن السيبراني مواعيد عمليات التفتيش والمراجعة على أساس سنوي بناءً على أهمية الجهات المعنية بالبنى التحتية للمعلومات الحيوية، ويحظى المجلس بدعم مجموعة عمل برنامج حماية البنى التحتية للمعلومات الحيوية واللجنة الوطنية لتوجيه الأمن السيبراني.

2.4.1.3 في حال اكتشاف حالات عدم الامتثال بالسياسات، تُصعّد هذه الحالات إلى مجموعة عمل البرنامج الوطني لحماية البنى التحتية للمعلومات الحيوية، ويُتوقع من مجلس الأمن السيبراني التدخل في المسائل التي قد تعرض الأمن السيبراني الوطني للخطر من خلال تطبيق العقوبات الإدارية، مثل: الغرامات وسحب الرخص التشغيلية أو أي إجراء آخر حسب الضرورة.

2.4.1.4 تُنفّذ الإجراءات الخاصة بمراقبة المخاطر وتقليص الأثر للجهات المعنية بالبنى التحتية للمعلومات الحيوية بما يتماشى مع الإطار الوطني لإدارة المخاطر السيبرانية.

2.4.1.5 يعمل مجلس الأمن السيبراني على نشر التوعية والفهم لدى الجهات المعنية حول طبيعة ما تملكه من بنى تحتية للمعلومات الحيوية، ودور كل جهة معنية وتوقعاتها في حماية البنى التحتية للمعلومات الحيوية والمساهمة في تعزيز مشهد الأمن السيبراني على المستوى الوطني.

2.4 ضمان برنامج حماية البنى التحتية للمعلومات الحيوية

2.4.2 المراقبة

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

قياس مدى فاعلية برنامج حماية البنية التحتية للمعلومات الحيوية في الإمارات العربية المتحدة وتحديد المشكلات المحتملة وتشجيع اتخاذ الإجراءات التحسينية.

بيانات السياسة

2.4.2.1 يعمل مجلس الأمن السيبراني على وضع الهياكل المؤسسية واتخاذ الإجراءات اللازمة لمراقبة فاعلية برنامج حماية البنى التحتية للمعلومات الحيوية ومستوى فعاليته، ولتتبع سير العمل لأنشطة البرنامج والتحقّق دورياً من تلبية متطلبات الأمن الوطني في القطاعات من قبل الجهات المعنية بالبنى التحتية للمعلومات الحيوية، وكل ذلك من خلال ما يلي:

- التقييم الذاتي للبنية التحتية للمعلومات الحيوية ورفع التقارير حول أداء خطة الجهة الخاصة ببرنامج حماية البنى التحتية للمعلومات الحيوية.
- رفع التقارير حول الخطط الموحّدة وسير الأنشطة لبرنامج حماية البنية التحتية للمعلومات الحيوية على مستوى القطاعات من قبل الجهة المسؤولة عن كل قطاع أو إمارة.
- وضع الخطة العامة لبرنامج حماية البنية التحتية للمعلومات الحيوية.
- إجراء مجلس الأمن السيبراني للمراجعات لغاية التحقّق من تقارير التقييم الذاتي.
- إجراء مجلس الأمن السيبراني اختبارات تدابير أمن المعلومات المنفذة.

2.4.2.2 يتعيّن على كافة الجهات المعنية بالبنى التحتية للمعلومات الحيوية إرسال أحدث المستجدات إلى مجلس الأمن السيبراني والجهات المنظّمة للقطاع بشأن سير خطة البنية التحتية للمعلومات الحيوية، وتقديم التقارير بخصوص التقييمات الذاتية، بالإضافة إلى المشاركة أثناء عمليات التدقيق وأنشطة الاختبار المجدولة وغير المجدولة. وفي الوقت الذي تستطيع فيه الجهات المعنية بالبنى التحتية للمعلومات الحيوية إجراء التقييمات الفنية الخاصة بها، إلّا أنه يجب إبلاغ مجلس الأمن السيبراني بأي أنشطة مجدولة على نحوٍ مسبق.

2.4.2.3 يسعى مجلس الأمن السيبراني إلى تطوير وتحسين برنامج حماية البنية التحتية للمعلومات الحيوية باستمرار، وذلك بناءً على مستوى الفاعلية الذي تُحدّده خطة البرنامج والمشهد العام للتهديدات وسجلات المخاطر.

2.4 ضمان برنامج حماية البنى التحتية للمعلومات الحيوية

2.4.3 الاعتماد

الإصدار 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

هدف السياسة

تمكين البنى التحتية للمعلومات الحيوية من التفاعل مع منظومة موثوق بها للحصول على خدمات الأمن السيبراني ورفع مستوى المعايير الأساسية في الإمارات العربية المتحدة في مجال الأمن الرقمي.

بيانات السياسة

2.4.3.1 سيعد مجلس الأمن السيبراني برنامج الاعتماد الذي سيساهم في تشجيع إيجاد إطار للاعتماد في مجال الأمن السيبراني داخل الدولة. وسيقوم المجلس بتوزيع لائحة تضم الجهات المعتمدة لتقديم الخدمات والبرامج التدريبية وعمليات التدقيق.

2.4.3.2 تخضع الجهات المعنية بالبنى التحتية للمعلومات الحيوية لعملية الاعتماد التي تستند إلى سجل المخاطر، إذ تُلزَم الجهات "ذات الخطورة العالية" بالالتزام بالبرنامج، بينما تُشجَع الجهات "ذات الخطورة المتوسطة أو المنخفضة" لاتباع المسار التطوعي المنصوص عليه في برنامج الاعتماد.

القسم 3

الملاحق

3.1 الوثائق المرجعية

معايير وسياسات دولة الإمارات العربية المتحدة

يوضّح الجدول التالي معايير وسياسات دولة الإمارات العربية المتحدة التي يستند إليها في تعريف بيانات هذه السياسة.

الهيئة/ الجهة	الوثيقة
مجلس الأمن السيبراني	الإطار الوطني للحوكمة
مجلس الأمن السيبراني	الإطار الوطني لضمان أمن المعلومات
مجلس الأمن السيبراني	قانون ضمان أمن المعلومات في دولة الإمارات العربية المتحدة.

3.1 الوثائق المرجعية

المعايير الدولية

يوضّح الجدول التالي المصادر الدولية المشار إليها في هذه الوثيقة.

الهيئة/ الجهة	الوثيقة
NIS2	مقترح لوضع توجيهات بخصوص التدابير المتعلقة بمستوى عالٍ من الأمن السيبراني عبر الدولة.
UNDRR	تعزيز البنى التحتية الحيوية لتصبح أكثر مرونة.
مؤسسة المنتدى العالمي للخبرات السيبرانية	دليل صنّاع السياسات GFCE-MERDIAN لأفضل الممارسات حول حماية البنية التحتية للمعلومات الحيوية.

3.2 الاختصارات

الهيئة/ الجهة	الوثيقة
CII	البنية التحتية للمعلومات الحيوية
CIIP	حماية البنية التحتية للمعلومات الحيوية
CSC	مجلس الأمن السيبراني
IT	تكنولوجيا المعلومات
ISO	المنظمة الدولية للمعايير
TLP	بروتوكول إشارات المرور
DNS	نظام أسماء النطاقات
IOT	إنترنت الأشياء
OT/ICS	التكنولوجيا التشغيلية وأنظمة التحكّم الصناعي
SOC	مراكز العمليات الأمنية

3.3 التعريفات

المصطلح	التعريفات
البنية التحتية الحيوية	تمثّل الأنظمة والأصول -سواء كانت مادية أو افتراضية- المهمة جداً بالنسبة لدولة الإمارات العربية المتحدة لدرجة أن إضعاف أو إتلاف هذه الأنظمة والأصول سيكون له أثر كبير على الأمن السيبراني أو الأمن الاقتصادي الوطني أو الصحة والسلامة العامة، أو مجموعة منها في آن واحد.
معلومات البنى التحتية الحيوية	أنظمة المعلومات، والأصول الرقمية، والشبكات، والخدمات، والتركيبات المترابطة التي تُستخدم لتقديم ودعم الخدمات الوطنية الحيوية في دولة الإمارات العربية المتحدة.
برنامج معلومات البنى التحتية الحيوية	آلية وإجراءات الحفاظ على المهام التشغيلية لنظم الاتصالات والمعلومات الأساسية للدولة دون وقوع المشكلات أو التعرض لها.
الأمن السيبراني	آلية وإجراءات حماية المعلومات من خلال منع الهجمات، واكتشافها، والاستجابة لها.
حدث الأمن السيبراني	تغيير في الأمن السيبراني قد يكون له أثر على العمليات التشغيلية للمؤسسات (بما يتضمن مهامها، وقدراتها، أو سمعتها).
حوادث الأمن السيبراني	حادث الأمن السيبراني الذي يجري تقييمه بأنه سيكون له أثرٌ على المؤسسة، مما يستدعي الاستجابة والتعافي منه.
الاكتشاف (وظيفة)	تطوير وتطبيق النشاطات والإجراءات المناسبة التي تعمل على تحديد حدوث حدث أمن سيبراني.
حادث الأمن الرقمي	حدث قد يشير إلى تعرض نظم تكنولوجيا المعلومات أو أي نظم رقمية أخرى لدى المؤسسة إلى الاختراق أو بأن إجراءات الأمان المتبعة والموضوعة لحماية هذه النظم قد فشلت في أداء وظيفتها.

3.3 التعريفات

المصطلح	التعريفات
الاحتواء	عملية الإبقاء على شيء ما ضار تحت السيطرة أو ضمن الحدود المقبولة.
الوقاية	الإجراءات التي يتم تطبيقها قبل وقوع حدث مهدد ما، والتي تهدف إلى التخفيف من و/ أو تجنب احتمالية وقوع أثر محتمل لأي حدث مهدد قد يكون ناجحاً.
مركز العمليات الأمنية	منشأة مراقبة مركزية يعمل فيها مجموعة من الأخصائيين ذوي الخبرة في مجال أمن المعلومات، والذين يقومون على مراقبة، وتحليل، وحماية المؤسسات من الهجمات السيبرانية.
أنظمة التحكّم الصناعية	مصطلح جامع يستخدم لوصف أنظمة التحكّم المتعددة وجميع الأدوات المرتبطة بها، والتي تتضمن الأجهزة، والأنظمة، والشبكات، والضوابط المستخدمة لإدارة و/ أو أتمتة العمليات الصناعية.
إنترنت الأشياء	نظام من أجهزة الحواسيب المترابطة، والآلات الميكانيكية والرقمية، والأشياء (المكونات)، والحيوانات أو الأشخاص الذين يتم تزويدهم بمعرِّفات فريدة، والقدرة على نقل البيانات عبر شبكة ما دون الحاجة إلى التدخل بنوعيه المتعلق بالبشر أو المرتبط بين البشر والآلات.
التمارين الطارئة	مجوعة الإجراءات التي تهدف إلى تحديد مدى وكيفية استجابة أي مؤسسة لحدث غير متوقع.
أمن سلسلة التوريد	يشكّل أمن سلسلة التوريد جزءاً من إدارة سلسلة التوريد والذي يركّز على إدارة المخاطر بخصوص المورّدين الخارجيين، ومقدّمي الخدمات العامة، وخدمات النقل، والخدمات اللوجستية.
المورّد المعتمد	المورّدون الموافق عليهم أو المعتمدون لتزويد المنتجات أو الخدمات.
نقطة التعطل المنفردة	خلل في تصميم، أو إعدادات، أو تطبيق النظام، أو الدارة، أو المكونات والتي تشكّل خطراً محتملاً قد يؤدي إلى وضع من المحتمل أن يكون فيه هذا الخلل الفردي مسؤولاً إن وقع تعطل عمل النظام بأكمله.

3.3 التعريفات

المصطلح	التعريفات
التهديدات	احتمالية قيام مصدر التهديد باستغلال الثغرات الأمنية بنجاح.
الثغرات الأمنية	نقطة ضعف في أصول المؤسسة، والتي من المحتمل أن تسمح بوقوع التهديد بصورة أكثر تكراراً، أو بمستوى أثر أكبر أو كليهما.
المخاطر	احتمالية أن يكون لوقوع الحدث تأثير سلبي على قدرة المؤسسة في تحقيق أهدافها.
الأزمة	حالة من الاضطراب أو التعطيل الشديد التي تهدد العمليات والأنشطة الأساسية.
المعلومات الحساسة	المعلومات الواردة ضمن مخطط التصنيف المتبع لدى دولة الإمارات العربية المتحدة، والتي قد تحدث ضرراً أو مشكلة، أو أنها قد تتسبب في وقوع الظلم على فرد أو مؤسسة في حال تم نشرها.
المعلومات الخاصة	المعلومات الواردة ضمن مخطط التصنيف المتبع لدى دولة الإمارات العربية المتحدة، والتي تُعد معلومات حساسة للغاية تملكها مؤسسة أو فرد ما ولا يجب نشرها للعامة.
المرونة	قدرة المؤسسة على التكيّف بسرعة مع الاضطرابات مع الحفاظ على سير الأعمال وحماية الأفراد والأصول والهوية المؤسسية العامة.
التبعية الرقمية والتبعيات المتبادلة	تتمثّل التبعية في "العلاقة بين منتجين أو خدمتين؛ بحيث يتطلب وجود منتج أو خدمة من أجل إنتاج المنتج أو الخدمة الأخرى"، أما التبعية المتبادلة فهي "تبعية المنتجات أو الخدمات على بعضها بشكل مشترك".
إطار العمل	منهج مبني على المخاطر يهدف إلى تقليص مخاطر الأمن السيبراني، ويتألف من ثلاثة أجزاء، وهي: أساس إطار العمل، ومواصفات إطار العمل، ومستويات تنفيذ إطار العمل. ويُعرف أيضاً باسم "إطار الأمن السيبراني".
مواصفات إطار العمل	النتائج التي اختارها نظام أو مؤسسة معينة من ضمن الفئات أو الفئات الفرعية الخاصة بإطار العمل.