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

الإمارات العربية المتحدة
وزارة شؤون مجلس الوزراء
مكتب رئاسة مجلس الوزراء

# البرنامج الوطني لاعتمادات الأمن السيبراني

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: | 15 مايو 2022 |
| جهة الإعداد: | مجلس الأمن السيبراني |
| التعديل: | وثيقة المسودة الأولية |

| الإصدار | 0.2 |
|---|---|
| التاريخ: | ... |
| جهة الإعداد: | ... |
| التعديل: | ... |

| الإصدار | 0.3 |
|---|---|
| التاريخ: | ... |
| جهة الإعداد: | ... |
| التعديل: | ... |

| | 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

تحرص دولة الإمارات العربية المتحدة على الاستمرار في تطوير ودعم بنيتها التحتية الرقمية ومجالها السيبراني، وذلك لدعم التنمية الاقتصادية وتوفير بيئة قادرة على حماية المصلحة العامة فيها. ويتمثّل الهدف من البرنامج الوطني لاعتمادات الأمن السيبراني في بناء الثقة بالمنظومة السيبرانية للدولة وذلك من خلال تعزيز القدرات الأمنية بوضوح وبشفافية تامة. ويعمل على الموازنة بين معايير الأمن والكفاءة وفقاً لأفضل الممارسات العالمية.

سيعمل البرنامج الوطني لاعتمادات الأمن السيبراني على تمكين الحكومة الإماراتية والجهات في الدولة من إثبات التزامها بالمعايير الأساسية للأمن السيبراني، بالإضافة إلى تمكينها من العمل مع الشركات والمؤسسات التي تلتزم بتطبيق هذه المعايير.كما ستوفّر تلك المعايير ضماناً للمعنيين بتطبيق هذه الجهات لأفضل الممارسات والتزامها بالحد الأدنى من مستوى الجاهزية في مجال الأمن السيبراني. مما يضمن ثبات مستوى خدمات الأمن السيبراني المقدّمة داخل الدولة.

## 1.1 الهدف

يتكون البرنامج الوطني لاعتمادات الأمن السيبراني من مساري اعتماد، ويوظف المعايير والضوابط الأمنية المعتمدة في ضمان أمن المعلومات في الدولة. تلزم جميع الجهات والمؤسسات الحكومية المشمولة في سياسة حماية البنية التحتية للمعلومات الحيوية، ومقدّمي الخدمات المتعاقدين مع الحكومة وكافة مقدّمي خدمات مجال الأمن السيبراني، من خدمات التدريب ،وخدمات التدقيق والمراجعة بالإضافة إلى الحصول على الاعتماد .في الوقت الذي يُعد الانضمام لهذا البرنامج اختيارياً بالنسبة للجهات الأخرى التي ترغب برفع قدرات برامج الأمن السيبراني لديها والحصول على الاعتمادات الموثوقة في هذا المجال.

يهدف إلى بناء الثقة بين الجهات الحاصلة على الاعتماد والمستخدمين والجهات المعنية (الملاك والشركاء والمواطنين، وغيرهم)، بالإضافة إلى رفع وتعزيز جاهزية الأمن السيبراني في الدولة. وسيطلق برنامج اعتماد المقيّمين المستقلين، والذين سيكون لهم دورٌ كبير في نشر وتطبيق البرنامج الوطني لاعتمادات الأمن السيبراني في كافة أنحاء الدولة. وتضمن هذه الوثيقة مكونات مختلفة من البرنامج الوطني لاعتمادات الأمن السيبراني، بما يتضمن التطبيق والصيانة، كما توفّر نظرة عامة شمولية لما يلي:

- عناصر البرنامج، بما يتضمن القدرات الوطنية، ونموذج عمل هذا الإطار وبرنامج اعتماد المقيّمين المستقلين ذي الصلة.
- المساران المحدّدان للحصول على الاعتماد وطرق التدقيق والحفاظ على الاعتماد، وعملية التقييم الذاتي والإطار الخاص بالضوابط الداعمة.
- تطبيق آلية المراقبة والتقييم على المستوى الوطني لضمان الالتزام المستمر بالمتطلبات وتنفيذ عملية قياس الأداء.

## 1.2 الجهة الوطنية المسؤولة

سيتم تعيين جهة وطنية مسؤولة عن إعداد البرنامج الوطني لاعتمادات الأمن السيبراني وتطبيقه والحفاظ عليه. الجهة الوطنية المسؤولة تمتلك الصلاحيات التنفيذية الكاملة للبرنامج، كما تمثّل نقطة التواصل المركزية على المستوى الوطني.

## 1.3 النطاق ومدى قابلية التطبيق

يطبّق البرنامج الوطني لاعتمادات الأمن السيبراني بشكل عام على جميع الجهات الحكومية ومؤسسات القطاع الخاص في الدولة، وكذلك على جميع الشركات والمؤسسات التي تقدّم الخدمات والجهات والمؤسسات الحكومية والخاصة التي تعمل في الخارج( من خلال برنامج المقيمين المستقلين)، سواءً بصورة إلزامية أو اختيارية.

- الجهات الحكومية: المؤسسات والجهات التي تُعتبر جزءاً من حكومة الدولة سواءً كانت دوائر حكومية أو شركات ومؤسسات تملكها أو تشغلها إحدى الجهات الحكومية في الدولة.
- البنية التحتية الحيوية: الجهات المحدّدة في سياسة حماية البنية التحتية للمعلومات الحيوية لدولة الإمارات العربية المتحدة.
- مقدّم خدمات الأمن السيبراني: يشير هذا المصطلح إلى جميع المؤسسات الموجودة في الدولة والتي تقدّم الخدمات التي تهدف إلى التقليل من المخاطر السيبرانية، والحماية من الهجمات السيبرانية والكشف عنها والاستجابة لها والتعافي منها، بما يتضمن شركات تقديم الخدمات التقنية والخدمات المُدارة وخدمات استشارات العمليات.
- مقدّم خدمات التدريب في مجال الأمن السيبراني: يشير هذا المصطلح إلى المؤسسات التي تقدّم الاعتمادات والشهادات المهنية للأفراد في الدولة.
- مقدّم خدمات التدقيق في مجال الأمن السيبراني: يشير إلى المؤسسات التي تقدّم خدمات التدقيق والمراجعة للجهات والمؤسسات في الدولة.
- الجهات الأخرى: أي جهة أو مؤسسة غير مشمولة في الفئات المعرفة أعلاه.

1. يُرجى الاطلاع على الملحق أ.

يتكون البرنامج الوطني لاعتمادات الأمن السيبراني من مساري اعتماد، أحدهما إلزامي والآخر اختياري (التقييم الذاتي)، وهو ما يجعله برنامجاً ثنائي المسار، إذ يتبع أسلوباً قائماً على المخاطر يسعى للموازنة بين المتطلبات الأمنية والكفاءة والفاعلية. وتطبّق هذه السياسة على النحو الآتي:

المسار الإلزامي: يتوجب على جميع الجهات الحكومية والمؤسسات التي تقدّم الخدمات إلى القطاع الحكومي في دولة الإمارات العربية المتحدة والمشمولة في سياسة حماية البنية التحتية للمعلومات الحيوية (خاصة مقدّمي خدمات الأمن السيبراني، ومقدّمي خدمات التدريب في مجال الأمن السيبراني، ومقدّمي خدمات التدقيق والمراجعة في مجال الأمن السيبراني) اتباع المسار الإلزامي الموضّح في البرنامج الوطني لاعتمادات الأمن السيبراني.

المسار الاختياري: يُمكن لأي جهة أو مؤسسة في دولة الإمارات العربية المتحدة المشاركة في البرنامج من خلال اتباع مسار التقييم الذاتي. ويُمكن لتلك الجهات والمؤسسات أن تقرر المشاركة في البرنامج وذلك لاستيفاء المتطلبات التنظيمية والتشريعية في الدولة (حسبما هو مذكور أعلاه) أو للحصول على إثبات رسمي لقبول واعتماد جاهزيتها في مجال الأمن السيبراني في كافة أنحاء الدولة.

يركّز البرنامج بصورة رئيسية على توفير المستوى الملائم من الضمان بناءً على قيمة المعلومات وطبيعة المخاطر المؤسسية، مستهدفاً بصورة أساسية الجهات الحكومية والجهات والمؤسسات التي تعمل مع الحكومة الإماراتية وقطاعات البنية التحتية للمعلومات الحيوية المشمولة.

ومن خلال عملية الاعتماد واتباع الأسلوب القائم على المخاطر، تسعى الجهات المعنية إلى رفع مستوى جاهزيتها في مجال الأمن السيبراني والتقليل من المخاطر السيبرانية، وهو ما يؤدي إلى وضع يتميّز بانخفاض التعرض الفردي للمخاطر السيبرانية ويساهم في دعم الجاهزية الوطنية لدولة الإمارات وبناء بيئة سيبرانية أكثر أمناً.

يجب أن يتوافق البرنامج الوطني لاعتمادات الأمن السيبراني مع السياسات الرئيسية الأخرى ذات العلاقة في الدولة. ويحتوي الملحق أ على قائمة بتلك السياسات المذكورة.

1. يُرجى الاطلاع على الملحق أ.

## 1.4 المبادئ التوجيهية

يستند البرنامج الوطني لاعتمادات الأمن السيبراني على مبادئ توجيهية معترف بها على الصعيد العالمي -أي مناهج حوكمة محدّدة- تهدف لإيجاد فهم مشترك بين الجهات المعنية في المجال السيبراني في الدولة. وعليه، فقد وُضعت جميع المبادئ التوجيهية أدناه بناءً على مجموعة الضوابط المتوافقة والمشمولة في لائحة ضمان أمن المعلومات في دولة الإمارات. وفيما يلي المبادئ المذكورة:

- التنظيم: تحديد المخاطر المتعلقة بالأمان وإدارتها.
- الحماية: تطبيق ضوابط الحماية للتقليل من المخاطر المتعلقة بالأمان.
- الكشف: فهم أحداث الأمن السيبراني وكشفها بما يُمكّن من تحديد حوادث الأمن السيبراني.
- الاستجابة: الاستجابة لحوادث الأمن السيبراني والتعافي منها.

مبادئ التنظيم

- UUAE-IA-M2: إدارة مخاطر أمن المعلومات
- UAE-IA-M5: الامتثال
- UAE-IA-T1: إدارة الأصول
- AE-IA-M1: الاستراتيجية والتخطيط

مبادئ الحماية

- UAE-IA-M3: التوعية والتدريب.
- UAE-IA-M4: أمن الموارد البشرية
- UAE-IA-M6: تقييم الأداء وتحسينه
- UAE-IA-T2: الأمن المادي والبيئي
- UAE-IA-T3: إدارة العمليات التشغيلية
- UAE-IA-T4: الاتصالات
- UAE-IA-T5: التحكّم بالوصول
- UAE-IA-T6: أمن الجهات الخارجية
- UAE-IA-T7: امتلاك وتطوير وصيانة أنظمة المعلومات

مبادئ الكشف

- UAE-IA-T3.6: المراقبة

مبادئ الاستجابة

- UAE-IA-T8: إدارة حوادث أمن المعلومات
- UAE-IA-T9: إدارة استمرارية عمل أنظمة المعلومات

## نموذج الجاهزية

عند تطبيق مبادئ الأمن السيبراني من خلال الضوابط المذكورة في ضمان أمن المعلومات في دولة الإمارات، تقيّم الجهة وفقاً لنموذج الجاهزية المذكور أدناه، وذلك لتقييم فاعلية تطبيق كل من تلك المبادئ بصورة منفردة، وعلى شكل مجموعة من المبادئ، بالإضافة إلى مبادئ الأمن السيبراني. وفيما يلي المستويات الأربعة لنموذج الجاهزية:

- **المستوى الأول: أولي**

امتثال محدودبالمبادئ التوجيهية أو بحسب الحاجة.

- **المستوى الثاني: متنامي**

يستوفي متطلبات الامتثال الأساسية وتتوفّر ضوابط دفاعية لمواجهة الهجمات الشائعة غير المستهدفة.

- **المستوى الثالث: متوسط**

يحقّق مستوى متوسط من الامتثال بالمتطلبات؛ تتوفّر ضوابط دفاعية لمواجهة الهجمات الشائعة والمستهدفة، حيث وضعت مبادئ الأمن السيبراني على أنها ممارسات عملية قياسية تنفّذ بشكل صارم على مستوى المؤسسة ككل.

- **المستوى الرابع: متقدّم**

مستوى عالي من الامتثال، حيث توجد ضوابط دفاعية لمواجهة العديد من التهديدات المستمرة والمتقدّمة. ويوجد تركيز مدروس على التحسين والتطوير المستمر لتطبيق مبادئ الأمن السيبراني على مستوى المؤسسة ككل.

## 1.5 الأهداف الاستراتيجية

يسعى البرنامج من خلال تحقيق الأهداف التالية إلى تعزيز ودعم بيئة الأمن السيبراني في دولة الإمارات العربية المتحدة:

| | |
|---|---|
| **إعداد إطار عمل خاص بدولة الإمارات العربية المتحدة** | **إعداد إطار عمل خاص بالدولة بحيث يستفيد من أنظمة وبرامج الاعتماد الدولية الموجودة والمعروفة في بناء وتعزيز سمعة الدولة كمركز عالمي للتميّز في خدمات الأمن السيبراني.** |
| **دعم تبنّي الضوابط الوطنية الموحّدة للأمن السيبراني** | يوظف البرنامج الوطني لاعتمادات الأمن السيبراني الضوابط الأمنية الموحّدة المذكورة في ضمان أمن المعلومات في دولة الإمارات، مما يضمن التطبيق المستمر للضوابط في جميع أنحاء الدولة ويقلل من احتمالية وجود أي ضوابط أو معايير متضاربة أو متناقضة. |
| **تمكين الجهات من التعامل مع الأمن السيبراني كأولوية مؤسسية باستخدام النهج القائم على المخاطر** | يتبع إطار العمل هذا نهجاً ذكياً قائماً على المخاطر لتحديد أولويات خدمات الأمن السيبراني حسب أهميتها بالنسبة للأمن الوطني لدولة الإمارات، والاعتراف بالجهات المعتمدة سعياً لتعزيز نمو منظومة الأمن السيبراني في الدولة.<br><br>وبصورة أساسية، يسعى النهج القائم على المخاطر إلى ربط مستويات المخاطر باستراتيجيات التخفيف المتوافقة معها، وذلك من أجل توفير نهج متوازن وفعّال من حيث التكلفة لأغراض الأمن السيبراني بحيث يوازن بين احتياجات الأعمال ومتطلبات الأمن السيبراني. |
| **دعم المسؤولية المشتركة ("توحيد الجهود")** | يجب أن تعمل الجهات المعنية في دولة الإمارات العربية المتحدة على توحيد الجهود ،وذلك لضمان فاعليتهم في الحفاظ على استقرار الفضاء السيبراني للدولة وقدرتهم على الاستثمار في الجهود التي تساهم في رفع مستوى جاهزية الأمن السيبراني فيها. وتتحمل الجهات والمؤسسات (خاصة مؤسسات تشغيل البنية التحتية الحيوية) والجهات المعنية على المستوى الوطني (أي الوزارات والجهات الحكومية) مسؤولية مشتركة في اتخاذ الخطوات الفعّالة للإسهام في تحقيق هذا الهدف. ويمثّل البرنامج الوطني لاعتمادات الأمن السيبراني إطار العمل الشامل الذي ينسق هذه المساعي الوطنية بهدف تحقيق أهدافه الطموحة على نحوٍ تعاوني وفعّال في بيئة معقدة تتألف من العديد من الجهات المعنية المختلفة. |

# القسم 2

## النموذج الوطني لحوكمة اعتمادات الأمن السيبراني

## 2.1.1 مسار الاعتماد الإلزامي

يتوجب على جميع الجهات الحكومية والمؤسسات المشمولة في سياسة حماية البنية التحتية للمعلومات الحيوية، والجهات التي تقدّم الخدمات للقطاع الحكومي (خاصة مقدّمي خدمات الأمن السيبراني، ومقدّمي خدمات التدريب في مجال الأمن السيبراني ومقدّمي خدمات التدقيق والمراجعة في مجال الأمن السيبراني) المشاركة في البرنامج إلزاميًا والحصول على المستوى المطلوب من اعتماد البرنامج الوطني لاعتمادات الأمن السيبراني والحفاظ عليه. كما يُمكن أن تكون المشاركة في البرنامج إلزامية بموجب القانون أو بناءً على طلب الجهات الحكومية ذات الصلة. ويتعلق ذلك على نحوٍ خاص ببرامج التعاون القائم بين القطاعين الحكومي والخاص أو برامج المشتريات، حيث يؤدي النهج القائم على المخاطر إلى فرض الاعتماد بموجب البرنامج الوطني لاعتمادات الأمن السيبراني.

لا تصدر شهادات اعتماد البرنامج الوطني لاعتمادات الأمن السيبراني إلّا من خلال الجهة الوطنية المسؤولة بعد الحصول على إثبات رسمي يبيّن نجاح الجهة في إكمال عملية التصديق والاعتماد. وتحتفظ الجهة الوطنية المسؤولة بقاعدة بيانات تضم الشهادات الصادرة (بما يتضمن تواريخ سريانها)، وتوفّر آلية لتمكين الجهات المعنية من التحقّق من تلك الاعتمادات.

صمّمت عملية التصديق والاعتماد لتنفّذها الجهة الوطنية المسؤولة باستخدام برنامج المقيّمين المستقلين باعتباره نهجاً مرناً وفعّالاً يُمكّنها من تقديم خدماتها بنجاح. ويسمح البرنامج بإدراج المؤسسات المهنية المؤهلة والأفراد الذين يمتلكون المهارات والموارد الضرورية وذلك لمصادقة امتثال الجهات لمتطلبات البرنامج الوطني لاعتمادات الأمن السيبراني. وهو ما يمكّن الجهة الوطنية المسؤولة من توظيف موارد القطاع الخاص من تطبيق البرنامج الوطني لاعتمادات الأمن السيبراني بنجاح من خلال اتباع نموذج يعزز ويضاعف من مستوى الفاعلية. ويحتوي الملحق ب على مخطط برنامج المقيّمين المستقلين.

ستُقاس مدى جاهزية الجهة وفقاً لنموذج الجاهزية الخاص بالبرنامج الوطني لاعتمادات الأمن السيبراني حسبما هو موضّح في القسم الخامس.

يهدف المسار الإلزامي إلى توفير الضمانات وطلب التزام الجهات المحدّدة في الدولة بضوابط الأمن السيبراني بناءً على ضمان أمن المعلومات لدولة الإمارات العربية المتحدة. ويطبّق المسار الإلزامي على الجهات الحكومية والمؤسسات المشمولة في سياسة حماية البنية التحتية للمعلومات الحيوية، والجهات التي تقدّم الخدمات للقطاع الحكومي (مقدّم خدمات الأمن السيبراني، ومقدّم خدمات التدريب في مجال الأمن السيبراني ومقدّم خدمات التدقيق والمراجعة في مجال الأمن السيبراني).

2. يُرجى الاطلاع على الملحق أ.

# 2.1.1 المسار الإلزامي

## 2.1.1.1 مقدّم خدمات الأمن السيبراني

يجب على الجهات التي تقدّم خدمات الأمن السيبراني للجهات الحكومية المحافظة على امتثالها لمتطلبات البرنامج الوطني لاعتمادات الأمن السيبراني.

وبالإضافة إلى ذلك، يجب أن يتمكّن مقدّم خدمات الأمن السيبراني من إثبات مستوى كفاءتهم في تقديم خدمات الأمن السيبراني التي يوفّرونها. فعلى سبيل المثال: يجب أن تكون الجهة التي تسعى إلى تقديم خدمات اختبار الاختراق لجهة حكومية قادرة على إثبات امتثالها لمتطلبات البرنامج الوطني لاعتمادات الأمن السيبراني، بالإضافة إلى إثبات امتلاك موظفيها المستوى المناسب من الكفاءة والمهارة، وذلك من خلال حصولهم على الاعتمادات المعترف بها في مجال عملهم، وبالمثل، يجب على الجهة التي تسعى إلى تقديم خدمات الاستجابة للحوادث لجهة حكومية إثبات كفاءتها وقدرتها على ذلك من خلال الحصول على الاعتمادات المناسبة.

4. يُرجى ملاحظة أن الملحق و: برنامج اعتمادات الأمن السيبراني - قائمة الاختيار (الجهات الحكومية والمؤسسات المعنية) يمثّل ملحقاً اختيارياً ضمن هذه الوثيقة.

# 2.1.1 المسار الإلزامي

## 2.1.1.2 مقدّم خدمات التدريب في مجال الأمن السيبراني

يجب على الجهات التي تقدّم خدمات التدريب في مجال الأمن السيبراني لصالح الجهات الحكومية الحفاظ على امتثالها لمتطلبات البرنامج الوطني لاعتمادات الأمن السيبراني.

بالإضافة إلى ذلك، يجب أن يتمكّن مقدّم خدمات التدريب في مجال الأمن السيبراني من إثبات كفاءتهم في مجال عملهم، ويجب أن تكون جهة معترف بها ومعتمدة لتقديم خدمات التدريب، كما يجب أن تتمكّن من إثبات امتلاك موظفيها للمستوى المناسب من الكفاءة في مجال التدريب الذي تقدّمه من خلالهم وحصولهم على الاعتمادات المطلوبة من الجهة المصممة للتدريب.

5. يُرجى ملاحظة أن الملحق و: برنامج اعتمادات الأمن السيبراني - قائمة الاختيار (الجهات الحكومية والمؤسسات المعنية) يمثّل ملحقاً اختيارياً ضمن هذه الوثيقة.

# 2.1.1 المسار الإلزامي

## 2.1.1.3 مقدّم خدمات التدقيق والمراجعة في مجال الأمن السيبراني

يجب على الجهات التي تقدّم خدمات التدقيق في مجال الأمن السيبراني للجهات الحكومية المحافظة على امتثالها لمتطلبات البرنامج الوطني لاعتمادات الأمن السيبراني.

بالإضافة إلى ذلك، يجب أن يتمكّن مقدّم خدمات التدقيق في مجال الأمن السيبراني من إثبات كفاءتهم في مجال عملهم. و الامتثال للمتطلبات الأساسية للبرنامج، كما يجب أن تثبت امتلاك موظفين الجهات للمستوى المناسب من الكفاءة من خلال حصولهم على المؤهلات المعترف بها في ذلك المجال.

6. يُرجى ملاحظة أن الملحق و: برنامج اعتمادات الأمن السيبراني - قائمة الاختيار (الجهات الحكومية والمؤسسات المعنية) يمثّل ملحقاً اختيارياً ضمن هذه الوثيقة.

## 2.1.2 مسار الاعتماد الاختياري (التقييم الذاتي)

يعمل مسار الاعتماد الاختياري من البرنامج الوطني لاعتمادات الأمن السيبراني على تمكين الجهات من المشاركة في البرنامج من خلال عملية التقييم الذاتي. ويتوفّر المسار الاختياري لكافة الجهات والمؤسسات غير المشمولة في سياسة حماية البنية التحتية للمعلومات الحيوية، أو التي يطلب منها الحصول على الاعتماد للعمل مع الحكومة. يُمكن لتلك الجهات والمؤسسات أن تقرر المشاركة في البرنامج وذلك لاستيفاء المتطلبات التنظيمية في الدولة تمهيداً لتقديم خدمات القطاع الحكومي أو لتقديم دليل على مستوى جاهزيتها في مجال الأمن السيبراني من خلال الحصول على اعتماد موثوق به يُمكنها الاستفادة منه مع الجهات المعنية فيها (أي ملاكها وشركائها، وعملائها، وما إلى ذلك).

يتطلب الحصول على الاعتماد القيام بعملية التقييم الذاتي، ويجب أن يوقعه الرئيس التنفيذي (أو ما يعادله) لمؤسسة القطاع الخاص بما يؤكد نزاهة وموثوقية عملية التصديق، ويجب أن تكون مسجله لدى الجهة الوطنية المسؤولة. وتصبح الجهات التي تنجح في إكمال عملية الاعتماد الذاتي مؤهلة للحصول على الاعتماد الاختياري من البرنامج الوطني لاعتمادات الأمن السيبراني، ويصدر تقرير الاعتماد الذاتي في البرنامج آلياً من قبل مجلس الأمن السيبراني .

بالإضافة لذلك، ستعمل الجهة الوطنية المسؤولة على التدقيق على الجهات الحاصلة على الاعتماد الذاتي عشوائياً من أجل التأكد من نزاهة العملية.

3

# القسم

## التطبيق

سيقود مجلس الأمن السيبراني في الدولة عملية تطبيق وتنفيذ البرنامج الوطني لاعتمادات الأمن السيبراني بصفته الجهة الوطنية المسؤولة عنه، بما يتضمن تصميم وتطبيق العمليات والإجراءات اللازمة لرفع قدرات وجاهزية البرنامج (بما يتضمن إطلاق برنامج المقيمين المستقلين).

كما ستضع الجهة الوطنية المسؤولة إجراءات الدعم والقدرات والأدوات والنظم والمحافظة عليها وتحديثها. وبناءً عليه، سيعمل مجلس الأمن السيبراني في دولة الإمارات العربية المتحدة مع الجهات الوطنية المعنية على تطبيق البرنامج الوطني لاعتمادات الأمن السيبراني لدولة الإمارات، وذلك لتوفير قدرات وطنية تشغيلية شاملة، والاستمرار في رفع جاهزيتها من خلال دورات مراجعة منظّمة لها.

# القسم 4

## أنشطة المراقبة وإدارة الأداء

يجب إعداد نظام مفصّل لمراقبة تنفيذ البرنامج الوطني لاعتمادات الأمن السيبراني كجزء من عملية تنفيذ البرنامج. وتُعتبر هذه الوظيفة التي تنفذها الجهة الوطنية المسؤولة ضرورية لجعل البرنامج قابلاً للقياس حيث تُعد القدرة على قياس برنامج الاعتماد ونتائجه ضرورية لبناء المعرفة فهي تعمل كأساس للتحسين والتطوير المستمر. ويجب أن تشتمل وظيفة المراقبة على مكونات متعددة، متضمنة إمكانية الاطلاع على التفاصيل والمؤشرات الرئيسية للجهات الخاضعة للتقييم، والإحصائيات حول الفجوات أو الثغرات التقليدية، بالإضافة إلى مؤشرات أخرى مماثلة (تجمع على أساس إحصائي مجهول الهوية) بحيث توضّح الجاهزية وقدرة القطاع أو المنظومة السيبرانية الإماراتية على المستويين الوطني والتراكمي. وتُعد تلك المعلومات الإحصائية بالغة الأهمية، فهي توفّر المعرفة بالوضع بشكل عام، وتمكّن من فهم الصورة الاستراتيجية لوضع الأمن السيبراني ومستوى جاهزيته، بالإضافة إلى المخاطر الأساسية واستراتيجيات الحد منها.

تشكّل إدارة الأداء وظيفة تابعة ومرتبطة بالبرنامج الوطني لاعتمادات الأمن السيبراني، حيث توظف البيانات المقدّمة من وظيفة المراقبة المذكور أعلاه، وتقارن تلك المُدخلات بمؤشرات الأداء الرئيسية المحدّدة مسبقاً لتوفير أساس موضوعي لتقييم الأداء الفعلي للبرنامج. ويُمكن التعرّف على مؤشرات الأداء الرئيسية ذات الصلة بناءً على المعايير العالمية التي توفّرها المصادر المهنية المتخصّصة في هذا المجال. ومن الناحية النظرية، يُمكن ربط تلك المؤشرات بتقييمات المخاطر ذات الصلة على المستوى الوطني، وتُعتبر بمثابة مُدخلات رئيسية لدعم أنشطة إدارة المخاطر والتحكّم بها. وفي نهاية المطاف، سيوفّر نظام إدارة الأداء الذي تحتفظ به الجهة الوطنية المسؤولة صورة واضحة حول كفاءة عمل النظام ومدى تحقيقه لأهدافه الرئيسية؛ وتطبّقه من خلال مؤشرات الأداء الرئيسية ذات الصلة، بحيث توفّر صورة واضحة حول التنفيذ وأساساً ثابتاً للتحسين المستمر للبرنامج.

5

# القسم

## الحصول على الاعتماد

## 5.1 نظرة عامة

يُمكن للجهات الحكومية الإماراتية والمؤسسات في الدولة الحصول على الاعتماد بموجب البرنامج الوطني لاعتمادات الأمن السيبراني من خلال نظام ثنائي المسار. وتُعتبر الجهات المحدّدة في السياسة ملزمة بالمشاركة في البرنامج، وتعمل الجهة الوطنية المسؤولة على تقييمها إما بصورة مباشرة أو من خلال إحدى الجهات الحكومية المفوضة بذلك، أو من خلال برنامج المقيّمين المستقلين. ويصدر الاعتماد الرسمي من الجهة الوطنية المسؤولة. ويحتوي الملحق ب على معلومات إضافية حول الجهات الحكومية المفوضة والمقيّمين المستقلين المعتمدين.

يُمكن لجميع الجهات والمؤسسات الأخرى في دولة الإمارات العربية المتحدة أن تقرر الحصول على الاعتماد من خلال عملية تقييم ذاتي اختيارية للتحقّق من مستوى جاهزيتها في مجال الأمن السيبراني، ولتحديد الفجوات ونقاط الضعف في بيئة التحكّم، ولإثبات إمكانياتها وقدراتها الأمنية السيبرانية للجهات المعنية بشأنها. كما يُمكن تنفيذ هذه العملية من خلال المقيّمين الخارجيين المشاركين في برنامج المقيّمين المستقلين.

# 5.2 العملية

## 5.2.1 مسار الاعتماد الإلزامي

يتوجب على جميع الجهات الحكومية والمؤسسات المشمولة في سياسة حماية البنية التحتية للمعلومات الحيوية، والجهات التي تقدّم الخدمات للقطاع الحكومي، وخاصة مقدّمي خدمات مجال الأمن السيبراني، المشاركة في البرنامج إلزاميًا والحصول على الاعتماد المطلوب من البرنامج الوطني لاعتمادات الأمن السيبراني والحفاظ عليه.

يجب على الجهات والمؤسسات الملتزمة بالبرنامج البدء بعملية اعتمادها من خلال التواصل مع الجهة الوطنية المسؤولة. وبدورها، ستعمل الجهة الوطنية المسؤولة على تنفيذ عملية التقييم باتباع إجراءات مفصّلة موضّحة في الإجراءات التشغيلية القياسية إما بصورة مباشرة أو من خلال إحدى الجهات الحكومية المفوضة بذلك، أو من خلال برنامج المقيّمين المستقلين.

تهدف عملية التصديق إلى تقييم الإثبات المقدّم من قبل الجهة مقابل الإطار الخاص بضوابط الاعتماد والمتوفّر كجزء من البرنامج الوطني لاعتمادات الأمن السيبراني (الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط). ويجب تنفيذ التقييم على نحوٍ موثّق حسبما هو محدّد في الإجراءات التشغيلية القياسية الخاصة بتقييم البرنامج. ويُمكن تحديد نطاق الضوابط غير المتعلقة بسياق الشبكات والأنظمة والأصول الخاصة بالجهة موضوع التقييم من خلال توفير أساس منطقي موثّق بما يتماشى مع متطلبات الإجراءات التشغيلية القياسية الخاصة بتقييم البرنامج الوطني لاعتمادات الأمن السيبراني.

ويجب أن تستكمل الجهة عملية التصديق في غضون 6 أشهر من تاريخ بدايتها. وفي حال العثور على بعض النواقص المهمة في الضوابط، يُمكن منح الجهة مهلة ثلاثة أو ستة أشهر لتصحيحها وتقديم إثبات بالتزامها بالضوابط المعنية. وفي حال عدم قدرة الجهة على تلبية هذا الاشتراط، عندها تُغلق عملية الاعتماد دون إصدار الشهادة.

تصدر الجهة الوطنية المسؤولة شهادة البرنامج الوطني لاعتمادات الأمن السيبراني في حال نجاح الجهة في إكمال عملية التصديق، وتمكّنها من توفير جميع الإثباتات المطلوبة لالتزامها بمتطلبات الإطار الوطني لضوابط اعتمادات الأمن السيبراني.

7. يُرجى الاطلاع على الملحق أ.

# 5.2 العملية

## 5.2.2 مسار الاعتماد الاختياري (التقييم الذاتي)

يُعتبر المسار الثاني من البرنامج الوطني لاعتمادات الأمن السيبراني مساراً اختيارياً، ويمثّل تأكيداً قائماً على التقييم الذاتي وتستطيع أي جهة أو مؤسسة في دولة الإمارات العربية المتحدة تنفيذه. تتألف هذه المجموعة من جميع الجهات غير المشمولة في سياسة حماية البنية التحتية للمعلومات الحيوية، أو التي يطلب منها الحصول على الاعتماد للعمل مع القطاع الحكومي (كما هو الحال بالنسبة لمقدّمي خدمات الأمن السيبراني، ومقدّمي خدمات التدريب في مجال الأمن السيبراني، ومقدّمي خدمات التدقيق في مجال الأمن السيبراني الذين يتعاقدون مع الجهات الحكومية لتقديم الخدمات)، حيث تستطيع هذه الجهات استخدام هذا المسار في حال رغبت بتقييم جاهزيتها في الأمن السيبراني، وتصحيح الفجوات وإثبات جهودها للجهات المعنية فيها بأنها عضو موثوق به من المنظومة السيبرانية في الدولة.

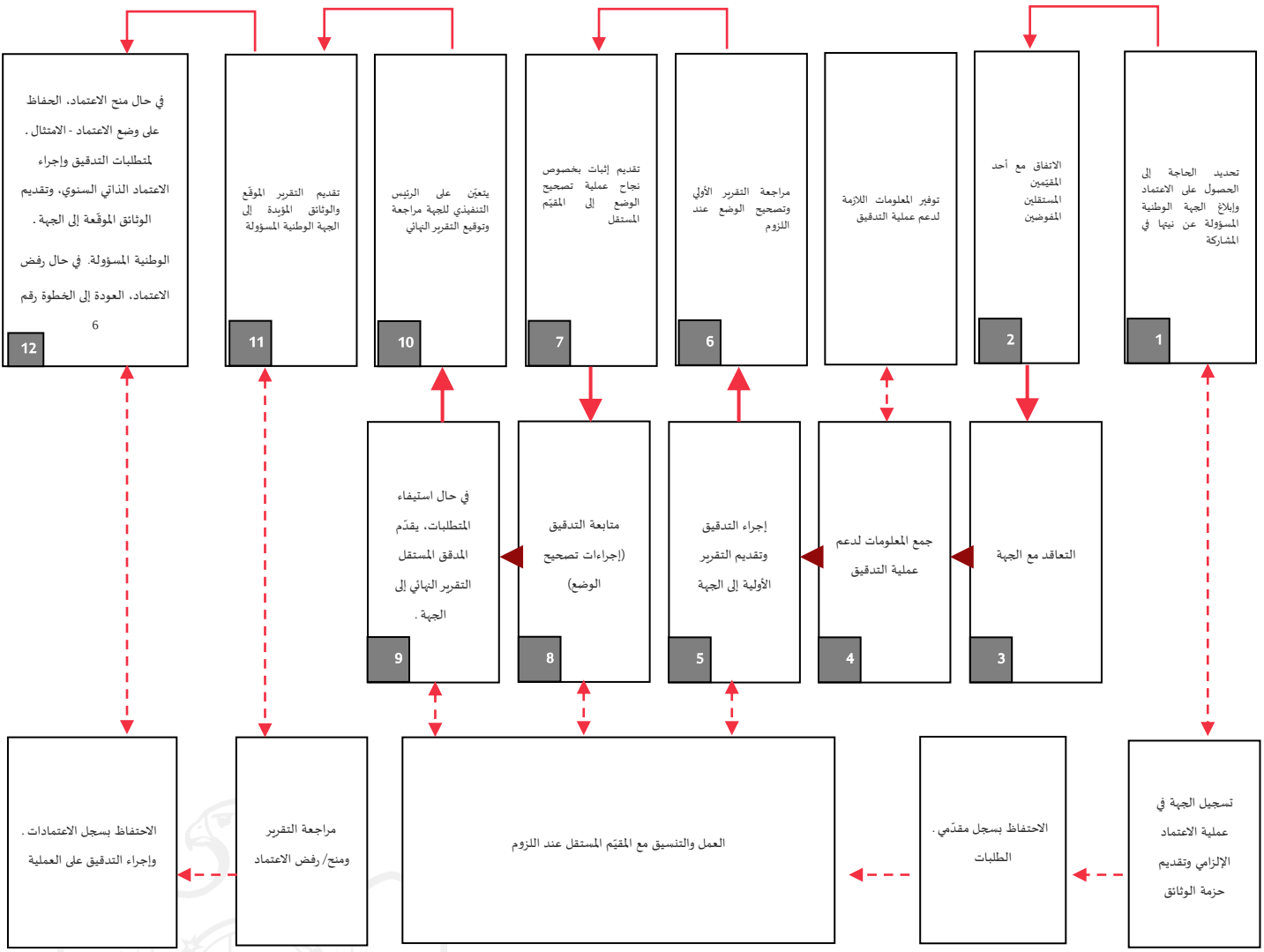
يتطلب الاكتمال الرسمي لعملية التقييم الذاتي توقيع الرئيس التنفيذي (أو ما يعادله) لمؤسسة القطاع الخاص على وثائق التقييم الذاتي للبرنامج الوطني لاعتمادات الأمن السيبراني، بما يؤكد نزاهة وموثوقية عملية التصديق.

تصبح الجهات التي تنجح في إكمال متطلبات عملية الاعتماد الذاتي مؤهلة للحصول على الاعتماد الاختياري من البرنامج الوطني لاعتمادات الأمن السيبراني، حيث يصدر تقرير الاعتماد الذاتي في البرنامج آلياً من قبل مجلس الأمن السيبراني .يُمكن للجهات المشاركة إثبات استيفائها لمتطلبات البرنامج الوطني لاعتمادات الأمن السيبراني من خلال عرض رمز إلكتروني للبرنامج الوطني لاعتمادات الأمن السيبراني على مواقعها الإلكترونية وعند طباعة المنشورات بما يتماشى مع المعايير التي يقررها مجلس الأمن السيبراني لدولة الإمارات العربية المتحدة.

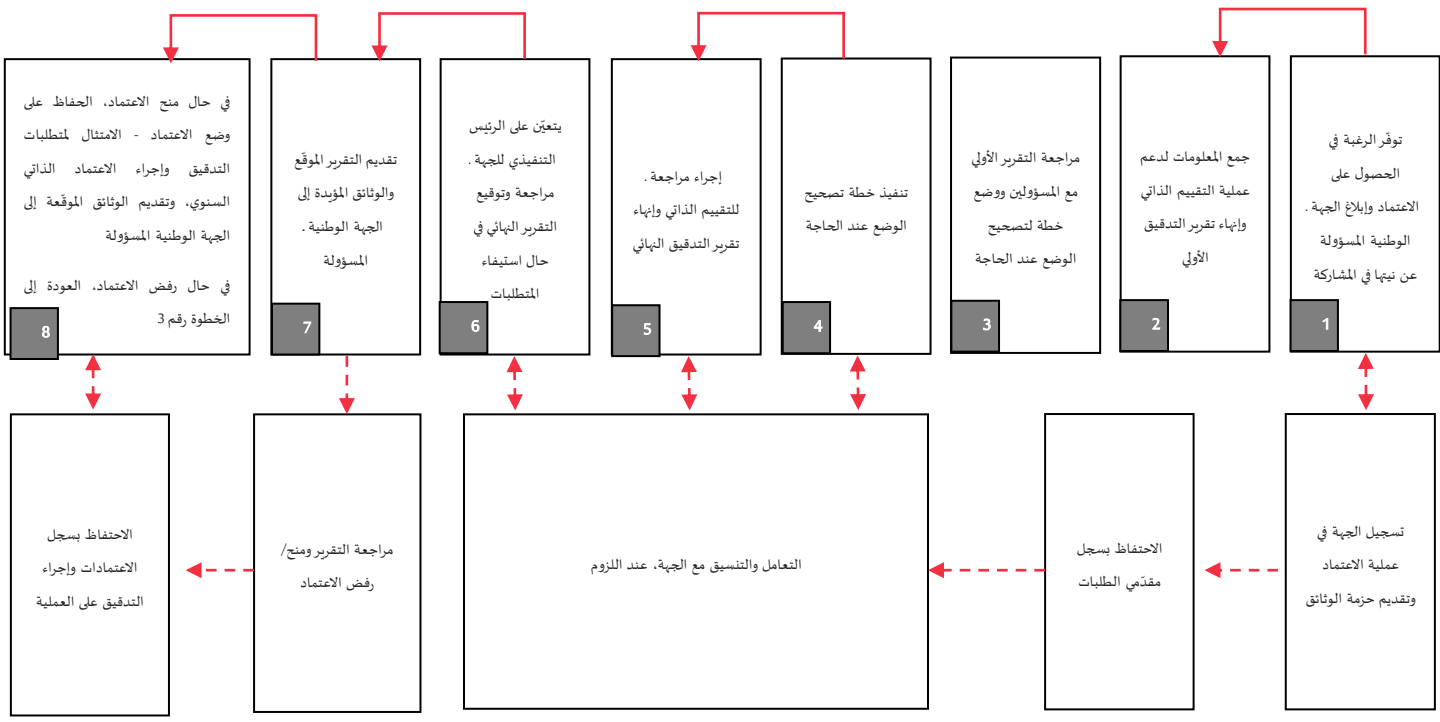
ويمكّن مسار الاعتماد الذاتي للبرنامج الوطني لاعتمادات الأمن السيبراني المؤسسات في المنظومة السيبرانية من تقييم وتعزيز وضعها في مجال الأمن السيبراني بفاعلية من حيث التكلفة، وإبلاغ الجهات المهنية فيها والمجتمع السيبراني الإماراتي الأوسع بالتزامها بتطبيق المعايير المحدّدة.

1. المقدّمة | 2. الإطار الوطني لاعتمادات الأمن السيبراني | 3. التنفيذ | 4. أنشطة المراقبة وإدارة الأداء | 5. الحصول على الاعتماد
6. التدقيق والحفاظ على الامتثال | 7. تطبيق الإطار الوطني لضوابط اعتمادات الأمن السيبراني | 8. الملاحق | 9. الملاحق الاختيارية

# 5.3 مخطط مسار الاعتماد الإلزامي



## 5.4 مخطط مسار الاعتماد الاختياري




يرجى الملاحظة: يُمكن للجهات المشتركة في الاعتماد الإلزامي التعاقد مع أحد المقيّمين المستقلين المفوضين لمساعدتها في العملية، على أن تقوم بذلك في الخطوة رقم 2 إن رغبت بذلك.

## 5.5 نموذج الجاهزية

ستكون للجهات مستويات مختلفة من متطلبات الجاهزية اعتماداً على نوع المعلومات المخزنة لديها، وقيمة المعلومات ووظيفة الجهة، وغيرها من العوامل الأخرى. ويحدّد نموذج الجاهزية الخاص بالبرنامج الوطني لاعتمادات الأمن السيبراني طريقة موحّدة لتتبع مستوى الجاهزية بين الجهات المختلفة. ولا يحل النموذج محل أي من المتطلبات المؤسسية الأخرى، ولكنه يوفّر طريقة خاصة بدولة الإمارات لقياس مستوى الجاهزية في مجال الأمن السيبراني. وستوفّر الجهة الوطنية المسؤولة دليلاً خاصاً لقياس مستوى جاهزية الجهات المختلفة عند تطبيق عملية الاعتماد وتنفيذها.

**مستويات نموذج الجاهزية في البرنامج**

| المستوى | ملاحظة حول الامتثال | الملاءمة |
|---|---|---|
| 1 | امتثال محدود أو بحسب الحاجة بالمبادئ التوجيهية. | ملائم فقط للجهات التي بدأت للتو في تطبيق إجراءات الأمن السيبراني. |
| 2 | يستوفي متطلبات الامتثال الأساسية وتتوفّر ضوابط دفاعية لمواجهة الهجمات الشائعة غير المستهدفة. | الحد الأدنى لمستوى الامتثال الملائم لأغلب الجهات غير الحكومية في الدولة. |
| 3 | يحقّق مستوى متوسط من الامتثال بالمتطلبات؛ تتوفّر ضوابط دفاعية لمواجهة الهجمات الشائعة والمستهدفة، حيث وضعت مبادئ الأمن السيبراني على أنها ممارسات عملية قياسية تنفّذ بشكل صارم على مستوى المؤسسة ككل. | الحد الأدنى لمستوى الامتثال الملائم لأغلب الجهات الحكومية في الدولة. |
| 4 | مستوى عالي من الامتثال، حيث توجد ضوابط دفاعية لمواجهة العديد من التهديدات المستمرة والمتقدّمة. ويوجد تركيز مدروس على التحسين والتطوير المستمر لتطبيق مبادئ الأمن السيبراني على مستوى المؤسسة ككل. | مستوى عالي من الامتثال وهو مناسب للحكومة أو الجهات التي تتعامل مع معلومات حساسة. |

## 5.6 الاعتراف المتبادل بالاعتمادات الموجودة

في بعض الحالات، يُمكن أن تكون الجهة التي تسعى إلى الحصول على الاعتماد الإلزامي أو الاختياري حاصلة على اعتماد وفق إحدى المعايير المعترف بها عالمياً. وفي هذه الحالة، يُمكن للبرنامج الوطني لاعتمادات الأمن السيبراني،، السماح للجهات التي تحمل الاعتمادات الموجودة الحصول على الاعتماد دون الخضوع لعملية التدقيق الكاملة.

للحصول على الاعتماد، يجب على الجهة تقديم ما يلي:

- إثبات رسمي بالاعتماد أو التوثيق الموجود
- وثائق مدقّقة تدعم الاعتماد أو التوثيق الموجود

بالإضافة لذلك، يجب أن تكون المجالات أو الأنظمة المطلوب اعتمادها من خلال البرنامج الوطني لاعتمادات الأمن السيبراني (أهداف التقييم) متطابقة مع تلك المعتمدة أو المقيّمة من خلال الاعتماد أو التوثيق المعترف به، على أن يغطي ذلك الاعتماد الموجود كافة الضوابط ذات الصلة المذكورة في البرنامج الوطني لاعتمادات الأمن السيبراني.

فيما يلي الاعتمادات والتوثيقات التي يُمكن الاعتراف بها ضمن البرنامج الوطني لاعتمادات الأمن السيبراني:

- CREST
- ISO27001
- NIST SP 800-53 REV. 5
- HIPAA
- معايير أمن البيانات في قطاع بطاقات الدفع (PCI-DSS)

# 5.6 الاعتراف المتبادل بالاعتمادات الموجودة

## 5.6.1 التقدّم للحصول على الاعتراف المتبادل

للتقدّم بالحصول على الاعتراف المتبادل لاعتماد، يجب على الجهة التواصل مع الجهة الوطنية المسؤولة بصورة مباشرة.

ويُمكن الاستفادة من الاعتراف المتبادل أيضاً لدعم جزءٍ من عملية الاعتماد في البرنامج الوطني لاعتمادات الأمن السيبراني، ويعني ذلك إذا كانت الجهة تستفيد من خدمة معتمدة أو موثّقة باستخدام اعتماد أو توثيق متبادل، يُمكن للمؤسسة التي تقدّم الخدمات لتلك الجهة أن تقدّم إثباتًا بالاعتماد أو التوثيق الموجود لإكمال جزء من نظام التقييم.

# القسم 6

## التدقيق والحفاظ على الامتثال

## 6.1 عملية التدقيق

كما هو موضّح بالتفصيل في نموذج إطار العمل، يُمكن للجهات الحكومية والمؤسسات في الدولة الحصول على الاعتماد بموجب البرنامج الوطني لاعتمادات الأمن السيبراني من خلال نظام ثنائي المسار. وتُعتبر الجهات المحدّدة في السياسة ملزمة بالمشاركة في البرنامج، وتعمل الجهة الوطنية المسؤولة على تقييمها إما بصورة مباشرة أو من خلال إحدى الجهات الحكومية المفوضة بذلك، أو من خلال برنامج المقيّمين المستقلين. وفي هذه الحالة، لا تصدر الاعتمادات الرسمية إلّا عن الجهة الوطنية المسؤولة فقط. ويجب تحديد طريقة التدقيق المفصّلة بما يتضمن نطاق التدقيق وإجراءاته، وعملية جمع الأدلة والاحتفاظ بها في وثيقة الإجراءات التشغيلية القياسية الصادرة عن الجهة الوطنية المسؤولة.

تُعد الجهة الوطنية المسؤولة مخططًا لبرنامج المقيّمين المستقلين المتعلق بالبرنامج الوطني لاعتمادات الأمن السيبراني حسبما هو مبيّن في الملحق ب.

وتوفّر الجهة الوطنية المسؤولة حزمة وثائق كاملة لمساري الاعتماد الإلزامي والاختياري عند التسجيل للبدء في عملية الاعتماد.

وفي الوقت ذاته، وحسبما هو موضّح بالتفصيل في نموذج إطار العمل، يُمكن للجهات والمؤسسات التي تزاول أعمالها في دولة الإمارات العربية المتحدة الحصول على الاعتماد بموجب البرنامج الوطني لاعتمادات الأمن السيبراني من خلال عملية اختيارية تتمثّل بإجراء التقييم الذاتي. ويجب تحديد تفاصيل تلك العملية في وثيقة الإجراءات التشغيلية القياسية من قبل الجهة الوطنية المسؤولة.

وكما هو محدّد أعلاه، يجب أن يوقع الرئيس التنفيذي (أو ما يعادله) لمؤسسة القطاع الخاص على الوثيقة، بحيث يتحمل المسؤولية القانونية الكاملة عن صحة ونزاهة عملية التقييم الذاتي، وبذلك تستكمل عملية الاعتماد. تُعد الجهة الوطنية المسؤولة برنامج رقابة خارجي يتسم بالدقة ويسعى إلى التدقيق على المشاركين في مسار الاعتماد الاختياري عشوائياً، وذلك لتوفير الرقابة والإشراف التنظيمي الفعّال، ولضمان الجودة ولمنع إساءة استخدام البرنامج. وسيكون تنفيذ برنامج الرقابة المذكور مدعوماً من قبل برنامج المقيّمين المستقلين.

## 6.2 الحفاظ على الامتثال

تنتهي صلاحية جميع اعتمادات المسار الإلزامي بعد ثلاث سنوات من صدورها، ولضمان تحقيق أهداف البرنامج الوطني لاعتمادات الأمن السيبراني المتمثّلة في توفير الضمانان اللازمة إلى كافة الجهات المعنية. ويُعتبر هذا الشرط ضرورياً بسبب التطوير والتغيير المتسارع الذي يشهده مجال التكنولوجيا وبيئات التهديد، كما سيتم التطرق إلى التغييرات الناتجة عن ذلك في لائحة ضمان أمن المعلومات في الدولة. وبناءً عليه، يجب أن يعكس البرنامج الوطني لاعتمادات الأمن السيبراني الطبيعة الديناميكية لمجال تكنولوجيا المعلومات ليوفّر ضماناً مجدياً للجهات المعنية في الدولة.

يجب استكمال عملية الاعتماد الإلزامي كل ثلاث سنوات للحفاظ على الامتثال والاستجابة للمتطلبات المتغيّرة التي تقررها الجهة الوطنية المسؤولة، وذلك من خلال إجراء التحديثات الدورية على الإطار الوطني لضوابط اعتمادات الأمن السيبراني. ويجب أن تأخذ قرارات تحديد النطاق بما يتماشى مع وثيقة الإجراءات التشغيلية القياسية المفصّلة التي تنشرها الجهة الوطنية المسؤولة في الاعتبار النتائج والأدلة المقدّمة خلال التقييمات السابقة بما يُمكّن من تسهيل وتبسيط العملية، عند الاقتضاء.

أما اعتمادات المسار الاختياري، فيتوجب استكمال إجراءاتها سنوياً.

كما يجب إعادة عملية الحصول على الاعتماد بموجب البرنامج الوطني لاعتمادات الأمن السيبراني في حال كان هناك تغيّر جوهري وكبير على البنية التحتية المعلوماتية أو الأساليب التكنولوجية أو العملياتية المتبعة (مثل: تغيير مقدّم خدمات البنية التحتية، أو في حال دمج الإدارات أو البرامج التقنية للشركات، أو في حال كانت هناك أي تغيّرات كبيرة أخرى تؤثر على الاعتبارات الأمنية المؤسسية).

يؤدي برنامج المقيّمين المستقلين دوراً مهماً وحيوياً في جهود الحفاظ على الامتثال المبذولة في الدولة وذلك بفاعلية من حيث التكلفة.

# القسم 7

تطبيق الإطار الوطني لضوابط اعتمادات الأمن السيبراني

يحتوي الملحق ج على الإطار الوطني لضوابط اعتمادات الأمن السيبراني

## 7.1 الحوكمة

يُعتبر الإطار الوطني لضوابط اعتمادات الأمن السيبراني من العناصر المهمة والضرورية للبرنامج الوطني لاعتمادات الأمن السيبراني، وبالتالي فهو ملكٌ للجهة الوطنية المسؤولة. ويجب أن يُراجع ذلك الإطار سنوياً على الأقل للتأكد من تحديثه واستيعابه للتغييرات وتوافقه مع التكنولوجيا وبيئات التهديد سريعة التغيّر.

يحتوي الملحق ج على الإطار الوطني لضوابط اعتمادات الأمن السيبراني

## 7.2 تطبيق الضوابط

تُعتبر معظم الضوابط المشمولة في الإطار الوطني لضوابط اعتمادات الأمن السيبراني الخاص بالبرنامج الوطني لاعتمادات الأمن السيبراني إلزامية (دائمة التطبيق) وذلك لضمان وجود حد أدنى من الالتزام بمعايير الأمن السيبراني في المنظومة السيبرانية. ومع ذلك، فإن وضع مجموعة فرعية من الضوابط يُعتبر اختيارياً (كما هو موضّح في هذه الوثيقة) للسماح باتخاذ قرارات تحديد النطاق الفردية بناءً على ملف المخاطر الخاص بالجهة الخاضعة للتقييم، وهو ما يعكس بيئات تكنولوجيا المعلومات الخاصة بها ويُمكّن من تقييم المخاطر التي تتعرض لها مع مراعاة أنشطة الجهة ومجال عملها. وتؤدي هذه الضوابط الاختيارية دوراً مهماً في التعامل مع المخاطر التي تتعرض لها الجهة، وعليه، ينبغي الاستفادة منها ومواءمتها بما يتوافق مع أفضل الممارسات في مجال عمل الجهة.

8

# القسم
# الملاحق

# 8.1 الملحق أ: الوثائق المرجعية: سياسات ومعايير دولة الإمارات العربية المتحدة[10]

### الاستراتيجية الوطنية للأمن السيبراني في دولة الإمارات العربية المتحدة

وثيقة استراتيجية أساسية تحدّد الرؤية الأمنية السيبرانية، والطموحات، والأساسات الاستراتيجية للتطبيق البرمجي، والأهداف والمتطلبات التنظيمية وقدرات التصور للمنظومة السيبرانية لدولة الإمارات العربية المتحدة.

### سياسة حماية البنية التحتية للمعلومات الحيوية (CIIP)

توضّح الأنشطة الذي سيستخدمها برنامج سياسة البنية التحتية للمعلومات الحيوية في تحديد قطاعات البنية التحتية الحيوية والخدمات الوطنية؛ وتحديد البنية التحتية للمعلومات التي تدعم الخدمات الوطنية الحيوية؛ ورفع المستويات الأمنية للبنى التحتية للمعلومات من خلال تطبيق المعايير والمتطلبات الأمنية السيبرانية اللازمة.

### إطار العمل الوطني لضمان أمن المعلومات (NIAF) ومعايير ضمان أمن المعلومات (IA)

يوضّح الإرشادات اللازمة لرفع مستويات الأمن السيبراني عبر جميع الجهات في الدولة من خلال المساعدة في إيجاد فهم مشترك حول متطلبات ضمان أمن المعلومات (IA) على مستوى الجهة ورفع المستويات الأمنية للبنية التحتية للمعلومات التي تدعم الخدمات الوطنية الحيوية من خلال دمج الجهات الفردية على المستوى الوطني ومستوى القطاع.

### إطار العمل الوطني لإدارة المخاطر السيبرانية (NCRMF)

يوضّح الأسلوب والمنهجية الوطنية المتبعة في تحديد وتقييم ومعالجة المخاطر الأمنية للبنية التحتية للمعلومات الحيوية.

### الإطار الوطني لمشاركة معلومات الأمن السيبراني (NCISF)

يحدّد الإطار الوطني لمشاركة معلومات الأمن السيبراني المتطلبات الرئيسية للتواصل بين الجهات والقطاعات ويُعد وسيلة داعمة لتطوير مستوى الوعي الوطني بالحالة السيبرانية.

### معايير الأمن السيبراني الصادر من مجلس الأمن السيبراني بقرار مجلس الوزراء رقم (8/8و) لسنة 2021

يحدّد معايير الأمن السيبراني المتطلبات الرئيسية لرفع المستوى الامن السبراني لدى الجهات و المؤسسات العاملة في الدولة ولتطوير مستوى الأمن السيبراني على الصعيد الوطني.

10. بناءً على المعلومات المتاحة.

# 8.2 الملحق ب: مخطط برنامج المقيّمين المستقلين

ستعد الجهة الوطنية المسؤولة برنامج المقيّمين المستقلين كمنهجية مرنة وفعّالة على مستوى الموارد، وذلك بهدف توسيع نطاق خدماتها وقدرتها على طرح البرنامج وإدارته. ويسمح برنامج المقيّمين المستقلين بإدراج المؤسسات المهنية المؤهلة والتي تم التحقّق منها ممن تمتلك المهارات والموارد الضرورية وذلك لمصادقة امتثال الجهات في الإمارات العربية المتحدة لمتطلبات البرنامج الوطني لاعتمادات الأمن السيبراني. وهو ما يمكّن الجهة الوطنية المسؤولة من توظيف موارد القطاع الخاص من تطبيق البرنامج الوطني لاعتمادات الأمن السيبراني بنجاح من خلال اتباع نموذج يعزز ويضاعف من مستوى الفاعلية. وسيساهم أيضاً المقيّمون المؤهلون المشاركون في برنامج المقيّمين المستقلين في الحفاظ على استقرار وأمن المجال السيبراني في دولة الإمارات العربية المتحدة من خلال دعم تطبيق مستوى أعلى من المعايير السيبرانية الأمنية عبر المنظومة السيبرانية للدولة.

بالإضافة إلى ذلك، قد تعمل الجهة الوطنية المسؤولة على تعيين جهات حكومية مفوضة تمتلك صلاحيات تنفيذ المراجعات والمصادقة بالنيابة عن الجهة الوطنية المسؤولة. ويجب على الجهات الحكومية المخوّلة الامتثال لمتطلبات برنامج المقيّمين المستقلين، وعلى طاقم الأفراد المشرف على إجراءات المراجعة ضمن الجهات الحكومية المخوّلة تلبية نفس المتطلبات المحدّدة للمقيّمين المستقلين المفوضين (كما يلي لاحقاً). كما ويجب نشر قائمة بالجهات الحكومية المفوضة من قبل الجهة الوطنية المسؤولة والمحافظة عليها.

10. بناءً على المعلومات المتاحة.

# 8.2 الملحق ب: مخطط برنامج المقيّمين المستقلين

قد يساعد المقيّمون المشاركون في برنامج المقيّمين المستقلين في تنفيذ تقييمات الجهات التابعة إلى المسار الإلزامي أو التحقّق منها ويُمكنهم أيضاً تقديم خدمات إضافية أو تنفيذ تقييمات للجهات من المسار الاختياري. ويجب أن تعد الجهة الوطنية المسؤولة الإجراءات التشغيلية القياسية بهدف تنظيم هذه الخدمات وتحديدها، بما يتضمن متطلبات تنفيذ التقييمات (وتشمل المتطلبات والمؤهلات العامة، وقواعد تحديد النطاق، وجمع الأدلة واستعادتها، والسرّية، والتواصل مع الجهة الوطنية المسؤولة، وما إلى ذلك).

كما يجب على الجهة الوطنية المسؤولة وضع معيار مفصّل أو إجراءات تشغيلية قياسية لمقيّمي البرنامج، بحيث تحدّد المجال والمعايير والأساليب المتبعة في اختبار أمن البيانات، والإجراءات التعاقدية ذات الصلة (ويشمل ذلك الاستبيانات، وغيرها). على مقدّمي خدمات الأمن السيبراني الذين يرغبون بالمشاركة في برنامج المقيّمين المستقلين الخضوع إلى عملية اختيار مناسبة تهدف إلى ضمان وجود إطار لمراقبة الجودة واستمرارية تنفيذ البرنامج. تهدف العملية إلى ضمان توظيف المقيّمين المشاركين لخبراتهم، وقدراتهم وكفاءاتهم الضرورية للعمل حسب متطلبات برنامج المقيّمين المستقلين. كما يجب أن تكون المتطلبات المحدّدة متوفّرة للجميع، ومن المهم أيضاً تشجيع المقيّمين المحتملين على التأكد من امتثالهم لها قبل تقديم طلباتهم.

# 8.2 الملحق ب: مخطط برنامج المقيّمين المستقلين

يجب أن تزود الجهة الوطنية المسؤولة المتقدّمين للحصول على رخصة باتفاقية عدم الإفصاح عن المعلومات وذلك لحماية سرّية إجراءات التقديم. ويُمكن النظر في وضع رسوم على تقديم هذا النوع من الطلبات وتوظيف المبالغ المحصلة لتغطية تكاليف عملية التقييم.

يتعيّن على المقيّمين المرخصين تجديد رخصتهم بانتظام (بعد مرور عام أو عامين).

ستضع الجهة الوطنية المسؤولة قائمة بالمقيّمين المرخصين المعتمدين من قبل برنامج المقيّمين المستقلين في قاعدة البيانات الرسمية والمحافظة عليها ونشرها للعامة. يجب أن توضّح الجهة الوطنية المسؤولة لأعضاء المنظومة السيبرانية في الدولة الذين يرغبون في الحصول على الاعتماد بأن المقيّمين المرخصين التابعين لبرنامج المقيّمين المستقلين هم الوحيدون المخوّلون للعمل في هذا المجال.

لضمان توفير خدمات عالية الجودة ومستوى عال من المساءلة، يجب أن يتم اعتماد الأفراد فقط بموجب برنامج المقيّمين المستقلين، على أن يستوفي الفرد الحد الأدنى من المتطلبات المتمثّلة بحصوله على إحدى المؤهلات المذكورة أدناه والحفاظ عليها، بالإضافة إلى امتلاكه 5 سنوات على الأقل من الخبرات المثبتة ذات الصلة.

**الشهادات**

**CISM - مدير معتمد في أمن المعلومات (جمعية التدقيق والرقابة على نظم المعلومات)**

**CISSP - شهادة أخصائي أمن نظم المعلومات المعتمد (2ISC)**

**CISA - مدقق نظم معلومات معتمد (جمعية التدقيق والرقابة على نظم المعلومات)**

**CRISC - الاعتماد في مجال ضوابط نظم المعلومات والمخاطر (جمعية التدقيق والرقابة على نظم المعلومات)**

**GSNA-GIAC - مدقق أنظمة وشبكات (SANS)**

**ISO 27001 - مدقق رئيسي (الرابطة العالمية لإدارة الجودة)**

**PCI QSA - مقيّم أمن معتمد من شركة متخصّصة في صناعة بطاقات الدفع (مجلس المعايير الأمنية)**

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني [5]. كما توفّر الجهة الوطنية المسؤولة حزمة وثائق كاملة للجهات التي تسعى إلى الحصول على الاعتماد خلال مرحلة التقديم الأولي على عملية الاعتماد.

## ضوابط الحوكمة

### 8.3.1 M1: الاستراتيجية والتخطيط

| M1 | الاستراتيجية والتخطيط |
|---|---|
| M1.1 | قيادة الجهة وسياق عملها |
| M1.1.1 | فهم الجهة وسياق عملها |
| M1.1.2 | التزام القيادة والإدارة |
| M1.1.3 | الأدوار والمسؤوليات المتعلقة بأمن المعلومات |
| M1.2 | سياسة أمن المعلومات |
| M1.2.1 | سياسة أمن المعلومات |
| M1.2.2 | دعم سياسات أمن المعلومات |
| M1.3 | أمن المعلومات في المؤسسات |
| M1.3.1 | عملية منح صلاحيات الوصول لأنظمة المعلومات |
| M1.3.2 | الاتفاقيات السرّية |
| M1.3.3 | التواصل مع الهيئات الحكومية |
| M1.3.5 | تحديد المخاطر المتعلقة بالجهات الخارجية |
| M1.3.7 | التطرق إلى العامل الأمني في الاتفاقيات مع الجهات الخارجية |
| M1.4 | الدعم (توفير الموارد) |
| M1.4.1 | توفير الموارد اللازمة |
| M1.4.2 | الاتصالات الداخلية والخارجية |
| M1.4.3 | التوثيق |

11. الإصدار 1.1، نشر في تاريخ مارس 2020.

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## ضوابط الحوكمة

### M2 8.3.2: إدارة مخاطر أمن المعلومات

| M2 | إدارة مخاطر أمن المعلومات |
|---|---|
| M2.1 | سياسة إدارة مخاطر أمن المعلومات |
| M2.1.1 | سياسة إدارة مخاطر أمن المعلومات |
| M2.2 | تقييم مخاطر أمن المعلومات |
| M2.2.1 | تحديد مخاطر أمن المعلومات |
| M2.2.2 | تحليل مخاطر أمن المعلومات |
| M2.2.3 | تقييم مخاطر أمن المعلومات |
| M2.3 | معالجة مخاطر أمن المعلومات |
| M2.3.1 | خيارات معالجة مخاطر أمن المعلومات |
| M2.3.2 | تحديد الضوابط |
| M2.3.3 | خطة معالجة المخاطر |

11. الإصدار 1.1، نشر في تاريخ مارس 2020.

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## ضوابط الحوكمة

### M3 8.3.3: التوعية والتدريب

| M3 | التوعية والتدريب |
|---|---|
| M3.1 | سياسة التوعية والتدريب |
| M3.1.1 | سياسة التوعية والتدريب |
| M3.2 | خطة التوعية والتدريب |
| M3.2.1 | برنامج التوعية والتدريب |
| M3.3.3 | تنفيذ التدريب |
| M3.4 | الوعي الأمني |
| M3.4.1 | حملة توعوية |

11. الإصدار 1.1، نشر في تاريخ مارس 2020.

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## ضوابط الحوكمة

### 8.3.4 M4: أمن الموارد البشرية

| M4 | أمن الموارد البشرية |
|---|---|
| M4.1 | سياسة أمن الموارد البشرية |
| M4.1.1 | سياسة أمن الموارد البشرية |
| M4.2 | أمن الموارد البشرية قبل التوظيف |
| M4.2.1 | التدقيق الأمني |
| M4.2.2 | شروط وأحكام التوظيف |
| M4.3 | خلال فترة التوظيف |
| M4.3.1 | المسؤوليات الإدارية |
| M4.3.2 | العملية التأديبية |
| M4.4 | إنهاء الخدمات أو تغيير الوظيفة |
| M4.4.1 | المسؤوليات المترتبة على إنهاء الخدمات |
| M4.4.2 | إعادة وتسليم الأصول |
| M4.4.3 | إيقاف صلاحيات الوصول |

11. الإصدار 1.1، نشر في تاريخ مارس 2020.

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## ضوابط الحوكمة

### 8.3.5 M5: الامتثال

| M5 | الامتثال |
|---|---|
| M5.1 | سياسة الامتثال |
| M5.1.1 | سياسة الامتثال |
| M5.2 | الامتثال للمتطلبات القانونية لأمن المعلومات |
| M5.2.1 | تحديد التشريعات المعمول بها |
| M5.2.3 | حماية السجلات المؤسسية |
| M5.2.4 | حماية البيانات وخصوصية المعلومات الشخصية |
| M5.2.6 | أحكام ضوابط التشفير |

11. الإصدار 1.1، نشر في تاريخ مارس 2020.

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## ضوابط الحوكمة

### 8.3.6 M6: تقييم الأداء وتحسينه

| M6 | تقييم الأداء وتحسينه |
|---|---|
| M6.1 | سياسة تقييم الأداء |
| M6.1.1 | سياسة تقييم الأداء |
| M6.2.1 | المراقبة والقياس والتحليل والتقييم |
| M6.2.2 | التدقيق الداخلي |
| M6.3.1 | الإجراءات التصحيحية |
| M6.3.2 | التحسين المستمر |

11. الإصدار 1.1، نشر في تاريخ مارس 2020.

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### T1 8.3.7: إدارة الأصول

| T1 | إدارة الأصول |
|---|---|
| T1.1 | سياسة إدارة الأصول |
| T1.1.1 | سياسة إدارة الأصول |
| T1.2 | المسؤوليات المتعلقة بالأصول |
| T1.2.1 | مخزون الأصول |
| T1.2.2 | ملكية الأصول |
| T1.2.3 | الاستخدام المقبول للأصول |
| T1.2.4 | الأصول المسموح باستخدامها، وإعدادات الأجهزة |
| T1.3 | تصنيف المعلومات |
| T1.3.1 | تصنيف المعلومات |
| T1.3.2 | علامات تصنيف المعلومات |
| T1.3.3 | التعامل مع أصول المعلومات |
| T1.4 | التعامل مع الوسائط |
| T1.4.1 | إدارة الوسائط القابلة للنقل |
| T1.4.2 | التخلص من الوسائط |

11. الإصدار 1.1، نشر في تاريخ مارس 2020.

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### 8.3.8 T2: الأمن المادي والبيئي

| T2 | الأمن المادي والبيئي |
|---|---|
| T2.1 | سياسة الأمن المادي والبيئي |
| T2.1.1 | سياسة الأمن المادي والبيئي |
| T2.2 | المناطق الآمنة |
| T2.2.1 | المحيط الأمني المادي |
| T2.2.2 | ضوابط الدخول المادية |
| T2.2.4 | الحماية من التهديدات الخارجية والبيئية |
| T2.2.5 (ضوابط اختيارية - بناءً على تقييم المخاطر) | العمل في المناطق الآمنة |
| T2.2.6 (ضوابط اختيارية - بناءً على تقييم المخاطر) | أماكن دخول عامة الأفراد وخدمات التوصيل والتحميل |
| T2.3 | أمن المعدات |
| T2.3.1 | مواقع المعدات وحمايتها |
| T2.3.2 | المرافق الداعمة |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### 8.3.8 T2: الأمن المادي والبيئي

| T2 | الأمن المادي والبيئي |
|---|---|
| T2.3.3 (ضوابط اختيارية - بناءً على تقييم المخاطر) | تأمين توصيل الأسلاك |
| T2.3.4 (ضوابط اختيارية - بناءً على تقييم المخاطر) | صيانة المعدات |
| T2.3.5 (ضوابط اختيارية - بناءً على تقييم المخاطر) | تأمين الحماية للمعدات الموجودة خارج المبنى |
| T2.3.6 | تأمين التخلص من المعدات أو إعادة استخدامها |
| T2.3.8 (ضوابط اختيارية - بناءً على تقييم المخاطر) | معدات المستخدم غير المراقبة |
| T2.3.9 (ضوابط اختيارية - بناءً على تقييم المخاطر) | سياسة المكتب النظيف والشاشة الخالية |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### 8.3.9 T3: إدارة العمليات التشغيلية

| T3 | إدارة العمليات التشغيلية |
|---|---|
| T3.1 | سياسة إدارة العمليات التشغيلية |
| T3.1.1 | سياسة إدارة العمليات التشغيلية |
| T3.2 | الإجراءات والمسؤوليات التشغيلية |
| T3.2.1 | الإرشادات المشتركة في إعداد الأنظمة |
| T3.2.2 | الإجراءات التشغيلية الموثّقة |
| T3.2.3 | إدارة التغيير |
| T3.2.4 | الفصل بين الواجبات |
| T3.2.5 | الفصل بين بيئات التطوير والاختبار والتشغيل |
| T3.3 | تخطيط النظام والقبول |
| T3.3.1 (ضوابط اختيارية - بناءً على تقييم المخاطر) | إدارة القدرات |
| T3.3.2 | إدارة القبول والاختبار |
| T3.4 | الحماية من البرمجيات الخبيثة |
| T3.4.1 | الضوابط المعنية بالبرمجيات الخبيثة |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### T3 8.3.9: إدارة العمليات التشغيلية

| T3 | إدارة العمليات التشغيلية |
|---|---|
| T3.5 | النسخ الاحتياطية |
| T3.5.1 | النسخ الاحتياطية للمعلومات |
| T3.6 | المراقبة |
| T3.6.1 | سياسات وإجراءات المراقبة |
| T3.6.2 | سجل التدقيق |
| T3.6.3 | مراقبة استخدام النظام |
| T3.6.4 | حماية معلومات السجل |
| T3.6.5 | سجلات الحسابات الإدارية والتشغيلية (حسابات مميّزة) |
| T3.6.6 | تسجيل الأخطاء |
| T3.6.7 | مزامنة الوقت |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### T4 8.3.10: الاتصالات

| T4 | الاتصالات |
|---|---|
| T4.1 | سياسة التواصل |
| T4.1.1 | سياسة التواصل |
| T4.2 | نقل المعلومات |
| T4.2.1 | إجراءات نقل المعلومات |
| T4.2.2 | اتفاقيات نقل المعلومات |
| T4.2.3 (ضوابط اختيارية - بناءً على تقييم المخاطر) | الوسائط المادية أثناء النقل |
| T4.2.4 | الرسائل الإلكترونية |
| T4.2.3 (ضوابط اختيارية - بناءً على تقييم المخاطر) | نظم المعلومات التجارية |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### T4 8.3.10: الاتصالات

| T4 | الاتصالات |
|---|---|
| T4.3 (ضوابط اختيارية - بناءً على تقييم المخاطر) | خدمات التجارة الالكترونية |
| T4.3.1 (ضوابط اختيارية - بناءً على تقييم المخاطر) | التجارة الالكترونية |
| T4.3.2 (ضوابط اختيارية - بناءً على تقييم المخاطر) | المعاملات عبر الانترنت |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### T4 8.3.10: الاتصالات

| T4 | الاتصالات |
|---|---|
| **T4.4 (ضوابط اختيارية - بناءً على تقييم المخاطر)** | حماية تبادل المعلومات |
| **T4.4.1 (ضوابط اختيارية - بناءً على تقييم المخاطر)** | الربط بمنصات تبادل المعلومات |
| **T4.4.2** | المعلومات المتاحة مع مجتمعات تبادل المعلومات |
| **T4.5** | إدارة أمن الشبكات |
| **T4.5.1** | ضوابط الشبكة |
| **T4.5.2** | أمن خدمات الشبكات |
| **T4.5.4** | أمن الشبكات اللاسلكية |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### 8.3.11 T5: التحكّم بالوصول

| T5 | التحكّم بالوصول |
|---|---|
| T5.1 | سياسة التحكّم بالوصول |
| T5.1.1 | سياسة التحكّم بالوصول |
| T5.2 | إدارة صلاحيات وصول المستخدم |
| T5.2.1 | تسجيل المستخدم |
| T5.2.2 | إدارة الوصول المتميّز |
| T5.2.3 | إدارة معلومات التعريف الأمنية للمستخدم |
| T5.2.4 (ضوابط اختيارية - بناءً على تقييم المخاطر) | مراجعة صلاحيات وصول المستخدم |
| T5.3 | مسؤوليات المستخدم (سياسات الاستخدام المقبولة) |
| T5.3.1 | استخدام معلومات التعريف الأمنية |
| T5.4 | التحكم بالوصول للشبكة |
| T5.4.1 | سياسة استخدام خدمات الشبكة |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### 8.3.11 T5: التحكّم بالوصول

| T5 | التحكّم بالوصول |
|---|---|
| T5.4.2 (ضوابط اختيارية - بناءً على تقييم المخاطر) | مصادقة وصول المستخدم في حال الاتصال من مواقع الخارجية |
| T5.4.3 | تعريف الأجهزة في الشبكات |
| T5.4.4 | التشخيص عن بُعد وضبط الإعدادات |
| T5.4.5 | التحكّم باتصال الشبكة |
| T5.4.6 | التحكّم بتوجيه الشبكة |
| T5.4.7 | الوصول اللاسلكي |
| T5.5 | التحكّم بالوصول إلى نظام تشغيل |
| T5.5.1 | إجراءات تسجيل الدخول الآمنة |
| T5.5.2 | تعريف ومصادقة المستخدم |
| T5.5.3 | نظام إدارة معلومات التعريف للمستخدم |
| T5.5.4 | استخدام أدوات النظام |
| T5.6 | التحكّم بالوصول إلى التطبيقات والمعلومات |
| T5.6.1 | تقييد الوصول للمعلومات |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### 8.3.12 T6: أمن الجهات الخارجية

| T6 | أمن الجهات الخارجية |
|---|---|
| T6.1 | سياسة أمن الجهات الخارجية |
| T6.1.1 | سياسة أمن الجهات الخارجية |
| T6.2 | إدارة تقديم الخدمات المتعلقة بالجهات الخارجية |
| T6.2.1 | تقديم الخدمات |
| T6.2.2 (ضوابط اختيارية - بناءً على تقييم المخاطر) | مراقبة ومراجعة الخدمات المتعلقة بالجهات الخارجية |
| T6.2.3 | إدارة التغييرات على الخدمات المتعلقة بالجهات الخارجية |
| T6.3 | الحوسبة السحابية |
| T6.3.1 | متطلبات أمن المعلومات للبيئات السحابية |
| T6.3.2 | اتفاقيات الخدمة مع مقدّمي خدمات الحوسبة السحابية |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### 8.3.13 T7: امتلاك وتطوير وصيانة أنظمة المعلومات

| T7 | امتلاك وتطوير وصيانة أنظمة المعلومات |
|---|---|
| T7.1 | سياسة امتلاك وتطوير وصيانة أنظمة المعلومات |
| T7.1.1 | سياسة امتلاك وتطوير وصيانة أنظمة المعلومات |
| T7.2 | المتطلبات الأمنية لأنظمة المعلومات |
| T7.2.1 | تحليل المتطلبات الأمنية وتحديدها |
| T7.3 (ضوابط اختيارية - بناءً على تقييم المخاطر) | العمليات الصحيحة في التطبيقات |
| T7.3.1 (ضوابط اختيارية - بناءً على تقييم المخاطر) | التحقّق من البيانات المُدخلة |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### T7 8.3.13: امتلاك وتطوير وصيانة أنظمة المعلومات

| T7 | امتلاك وتطوير وصيانة أنظمة المعلومات |
|---|---|
| T7.3.2 (ضوابط اختيارية - بناءً على تقييم المخاطر) | التحكّم بالعمليات الداخلية |
| T7.3.3 (ضوابط اختيارية - بناءً على تقييم المخاطر) | سلامة الرسالة |
| T7.3.4 (ضوابط اختيارية - بناءً على تقييم المخاطر) | التحكّم بالبيانات المُخرجة |
| T7.4 | ضوابط التشفير |
| T7.4.1 | سياسة استخدام ضوابط التشفير |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### T7 8.3.13: امتلاك وتطوير وصيانة أنظمة المعلومات

| T7 | امتلاك وتطوير وصيانة أنظمة المعلومات |
|---|---|
| T7.4.2 | إدارة المفاتيح |
| T7.5 | أمن ملفات النظام |
| T7.5.1 | التحكّم بالبرنامج التشغيلي (بيئة الإنتاج) |
| T7.5.2 | حماية بيانات اختبار النظام |
| T7.5.3 (ضوابط اختيارية - بناءً على تقييم المخاطر) | التحكّم بالوصول إلى الكود المصدري |
| T7.6 | الأمن في عمليات التطوير والدعم |
| T7.6.1 | إجراءات ضبط التغيير |
| T7.6.2 | المراجعة التقنية للتطبيقات بعد إجراء تغييرات على نظام التشغيل |
| T7.6.3 | فرض قيود على صلاحيات تغيير حزم البرامج |
| T7.6.4 | تسرب المعلومات |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### T7 8.3.13: امتلاك وتطوير وصيانة أنظمة المعلومات

| T7 | امتلاك وتطوير وصيانة أنظمة المعلومات |
|---|---|
| T7.6.5 (ضوابط اختيارية - بناءً على تقييم المخاطر) | تطوير البرمجيات من قبل مصادر خارجية |
| T7.7 | إدارة الثغرات الفنية |
| T7.7.1 | التحكّم بالثغرات الفنية |
| T7.8 | إدارة سلسلة التوريد |
| T7.8.1 | استراتيجية حماية سلسلة التوريد |
| T7.8.2 | مراجعة المورّدين |
| T7.8.3 | الحد من الأضرار |
| T7.8.4 | أمن عمليات سلسلة التوريد |
| T7.8.6 | عمليات معالجة نقاط الضعف أو الثغرات |
| T7.8.7 | مورّد مكونات نظام المعلومات الحيوية |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### T8 8.3.13.1: إدارة حوادث أمن المعلومات

| T8 | إدارة حوادث أمن المعلومات |
|---|---|
| T8.1 | سياسة إدارة حوادث أمن المعلومات |
| T8.1.1 | سياسة إدارة حوادث أمن المعلومات |
| T8.2 | إدارة حوادث أمن المعلومات وتحسينها |
| T8.2.1 | خطة الاستجابة للحوادث |
| T8.2.2 | فريق الاستجابة لحوادث أمن الحاسوب |
| T8.2.4 | تدريب الاستجابة للحوادث |
| T8.2.5 | اختبار الاستجابة للحوادث |
| T8.2.6 (ضوابط اختيارية - بناءً على تقييم المخاطر) | المساعدة في الاستجابة للحوادث |
| T8.2.7 | توثيق حوادث أمن المعلومات |
| T8.2.8 | التعلّم من حوادث أمن المعلومات |
| T8.2.9 | جمع الأدلة |
| T8.3 | الإبلاغ عن أحداث أمن المعلومات ونقاط الضعف |
| T8.3.1 | الوعي بالموقف العام |
| T8.3.2 | الإبلاغ عن أحداث أمن المعلومات |

# 8.3 الملحق ج: الإطار الوطني لضوابط اعتمادات الأمن السيبراني - قائمة الضوابط

يتوافق إطار ضوابط اعتمادات الأمن السيبراني مع ضمان أمن المعلومات للدولة[11].

## الضوابط التقنية

### 8.3.14 T9: إدارة استمرارية عمل أنظمة المعلومات

| T9 | إدارة استمرارية عمل أنظمة المعلومات |
|---|---|
| T9.1 | سياسة إدارة استمرارية عمل أنظمة المعلومات |
| T9.1.1 | سياسة التخطيط لاستمرارية عمل أنظمة المعلومات |
| T9.2 | جوانب أمن المعلومات في إدارة استمرارية المعلومات |
| T9.2.1 | وضع خطط استمرارية أنظمة المعلومات |
| T9.2.2 | تنفيذ خطط استمرارية أنظمة المعلومات |
| T9.3 | اختبار الخطط والمحافظة عليها وإعادة تقييمها |
| T9.3.1 | اختبار خطط استمرارية أنظمة المعلومات والمحافظة عليها وإعادة تقييمها |

# 8.4 الملحق د: الاختصارات

| الاختصارات | التعريفات |
|---|---|
| CIIP | سياسة حماية البنية التحتية للمعلومات الحيوية لدولة الإمارات |
| CIRT | فريق الاستجابة لحوادث أمن الحاسوب |
| CSC | مجلس الأمن السيبراني لدولة الإمارات العربية المتحدة |
| IAP | برنامج المقيّمين المستقلين |
| IA | ضمان أمن المعلومات |
| NCAP | البرنامج الوطني لاعتمادات الأمن السيبراني |
| NDA | اتفاقية عدم الإفصاح عن المعلومات |
| NSOC | المركز الوطني للعمليات الأمنية السيبرانية |
| SOC | مركز العمليات الأمنية |
| SOP | الإجراءات التشغيلية القياسية |