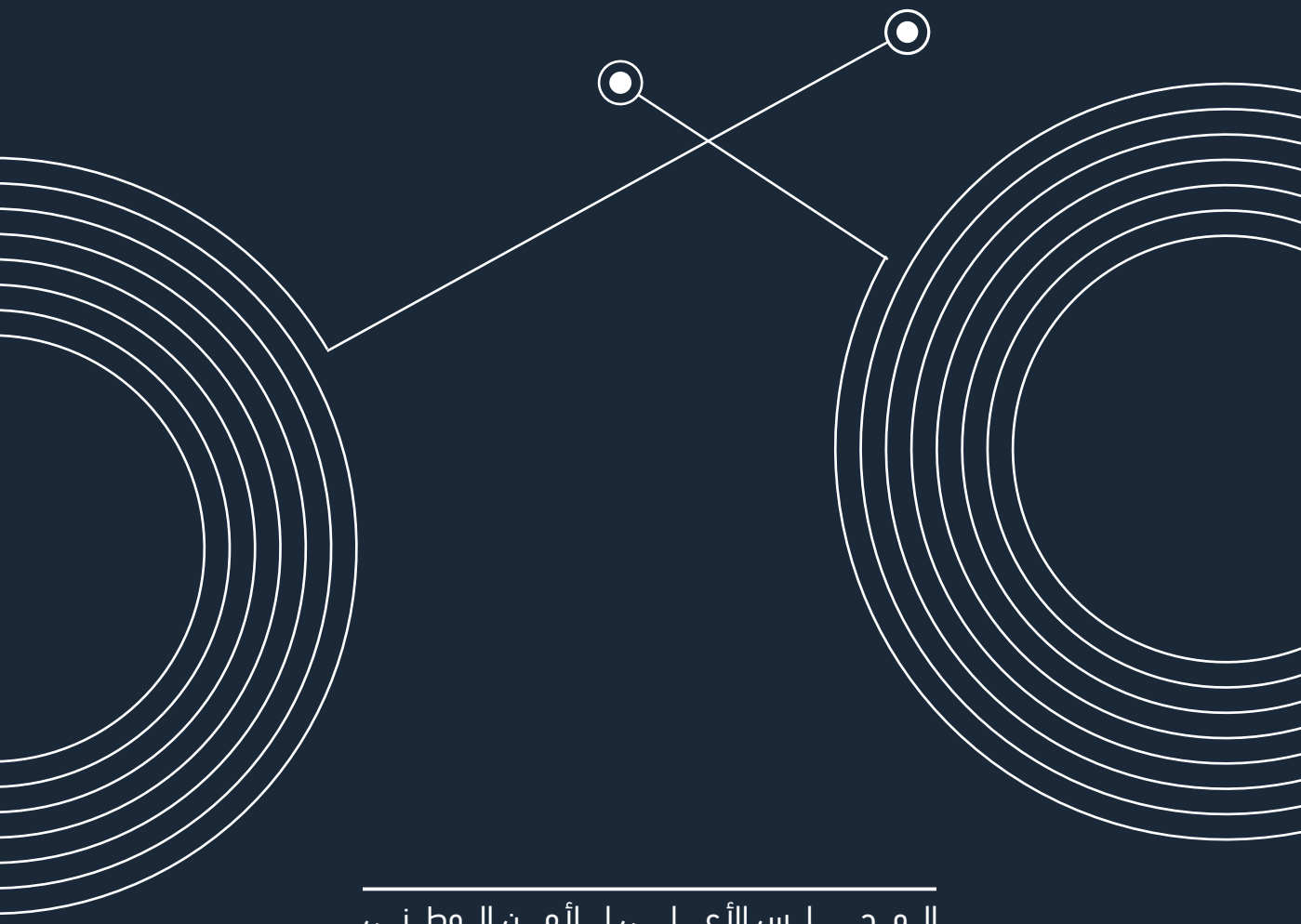
الهيئة الوطنية للأمن الإلكتروني
NATIONAL ELECTRONIC SECURITY AUTHORITY
الإمارات العربية المتحدة UNITED ARAB EMIRATES

سياسة حماية البنية التحتية للمعلومات الحيوية



المجلس الأعلى للأمن الوطني

جدول المحتويات

تمهيد

سعياً منا لتحقيق رؤية الإمارات العربية المتحدة الرامية إلى إيجاد مجتمع واقتصاد قادرين على المنافسة والصمود في خضم عصر المعلومات الذي نعيشه اليوم، فإنه لحري بنا الاستفادة من منافع الفضاء الإلكتروني والعمل على تبنيه وتمكينه، فهو يُشكل حجر الزاوية لمجتمع يساهم في تعزيز ثقافة نابضة والارتقاء بمستوى المعيشة للمواطنين والمقيمين على حد سواء. ومما لا شك فيه أن الأهمية الاستراتيجية للفضاء الإلكتروني ستستمر في النمو وسيزيد اعتمادنا الجماعي عليه ما يجعل منه أولوية محورية لبلادنا.

وعلى الرغم من كل هذه المنافع، فإن الاعتماد على الفضاء الإلكتروني تصاحبه مجموعة من التهديدات الإلكترونية سريعة التطوّر بما في ذلك الأنشطة الضارة التي من شأنها التأثير سلباً في سير العمل لدى الجهات الحكومية وقطاعات الأعمال وحياة المواطنين والمقيمين. ويمكن لتلك المخاطر أن تعيق قدرتنا على الاستفادة من المنافع والفرص الاجتماعية والاقتصادية التي يوفرها الفضاء الإلكتروني لشعبنا، كما يمكن أن تهدد أمننا الوطني.

وعلى الرغم من خطواتنا المحرزة في حماية بلادنا من هذا النوع الجديد من التهديدات فإنه لا يجب أن نتوانى عن بذل المزيد من الجهد من أجل مواصلة المسيرة، لأن مخاطر الفضاء الإلكتروني آخذة في الانتشار والتطوّر يوماً بعد يوم. لذا يجدر بنا تنسيق وتنظيم جهودنا بُغية الحفاظ على أمن الفضاء الإلكتروني في بلادنا.

وبناءً على ما سبق، قامت حكومة دولة الإمارات العربية المتحدة بإنشاء الهيئة الوطنية للأمن الإلكتروني لتُوكل إليها مهمة تعزيز الأمن الوطني من خلال الارتقاء بمستوى حماية البنية التحتية الوطنية لشبكة الاتصالات ونظم المعلومات بالاعتماد على أفضل السياسات والإجراءات وأحدث التقنيات الفائقة والموارد البشرية الخبيرة وزيادة الوعي لدى الجمهور، وكذلك من أجل توحيد وتوجيه الجهود الوطنية المبذولة في هذا الصدد.

وترسم استراتيجية دولة الإمارات العربية المتحدة للأمن الإلكتروني، الموضحة هنا في هذه الوثيقة التي أعدتها الهيئة الوطنية للأمن الإلكتروني، مسار التزام حكومتنا الدؤوب بحماية الفضاء الإلكتروني في وطننا. وستقوم الهيئة الوطنية للأمن الإلكتروني بمسؤولية تفعيل الاستراتيجية والإشراف على حوكمتها والتنسيق فيما بين جميع الجهات المعنية بحسب الأنشطة الخاصة بها.
وفي حين تبذل حكومتنا ما في وسعها لضمان أمن ومرونة الفضاء الإلكتروني في بلدنا، فإن مسؤولية المحافظة على الأمن الإلكتروني تبقى مسؤولية مشتركة بين كافة فئات المجتمع من حكومة ومؤسسات وأفراد. كما أن التعاون والشراكة على الصعيدين الوطني والإقليمي هما عماد النجاح في تحقيق هذه المهمة الوطنية والعالمية. وإنني على يقين بأن تضافر جهودنا جميعاً سيثمر عنه تحقيق الأهداف الوطنية للأمن الإلكتروني وحماية مصالح بلادنا.

جاسم بوعتابة الزعابي
المدير العام

الهيئة الوطنية للأمن الإلكتروني

الفصل الأول

مقدمة

١,١ الغاية

تسعى حكومة دولة الإمارات العربية المتحدة بصفتها راعية لأمن وسلامة الوطن، إلى مواجهة تحديات الأمن الإلكتروني بُغية تعزيز الثقة والمصداقية في المجتمع الرقمي ومجتمع المعلومات ودفع عجلة النمو الاقتصادي في دولة الإمارات. وبناءً على المرسوم الاتحادي رقم ٣ لسنة ٢٠١٢ (وتعديلاته)، قامت حكومة دولة الإمارات بتأسيس الهيئة الوطنية للأمن الإلكتروني لتوكل إليها مهمة تعزيز الأمن الوطني للدولة من خلال الارتقاء بمستوى حماية البنية التحتية الوطنية لشبكة الاتصالات ونظم المعلومات بالاعتماد على أفضل السياسات والإجراءات وأحدث التقنيات الفائقة والموارد البشرية الخبيرة وزيادة الوعي لدى الجمهور، وكذلك من أجل توحيد وتوجيه الجهود الوطنية المبذولة في هذا الصدد.

وترسم الاستراتيجية الوطنية للأمن الإلكتروني لدولة الإمارات، التي تشرف على حوكمتها ومتابعة تنفيذها الهيئة الوطنية للأمن الإلكتروني، مسار التزام الحكومة وسعيها الجاد والدؤوب لحماية الفضاء الإلكتروني في دولة الإمارات، حيث تعرض المجالات الاستراتيجية التي ينبغي أن تركز عليها دولة الإمارات للحفاظ على الأمن الإلكتروني الوطني، والأهداف الخاصة التي تندرج ضمن كل مجال من مجالات التركيز فضلاً عن خطة عامة لتحقيق تلك الأهداف.

وتدعم سياسة دولة الإمارات لحماية البنية التحتية للمعلومات الحيوية الموضحة في هذه الوثيقة تنفيذ الاستراتيجية الوطنية للأمن الإلكتروني. كما تعرض السياسة أنشطة برنامج حماية البنية التحتية للمعلومات الحيوية المقرر تطبيقه من أجل إنجاز ثلاثة أهداف محورية وهي:

- تحديد القطاعات والخدمات الوطنية الحيوية.
- تحديد البنى التحتية للمعلومات الداعمة للخدمات الوطنية الحيوية.
- الارتقاء بمستويات أمن تلك البنى التحتية من خلال تطبيق معايير ومتطلبات إلزامية للأمن الإلكتروني.

١,٢

أهمية حماية البنية التحتية للمعلومات الحيوية

البنية التحتية للمعلومات الحيوية عبارة عن أصول المعلومات المادية والافتراضية التي تدعم تنفيذ وظيفة بالغة الأهمية وتقديم خدمة حيوية على مستوى القطاع أو على المستوى الوطني. وتمثل هذه البنية التحتية حجر الزاوية لسير عمل المجتمع الإماراتي واقتصاده وتوفير خدمات دعم تعتمد عليها حكومة دولة الإمارات والمواطنون وقطاعات الأعمال. وبينما تُعد تلك البنية في أغلب الأحيان البنية التحتية الأساسية لجميع قطاعات الاقتصاد على غرار الاتصالات والخدمات المالية، فهي أيضاً جزء لا يتجزأ من بنى تحتية أكثر تعقيداً، مثل مرافق إمداد الكهرباء ونظم النقل الجوية والبحرية ومرافق المياه.

الجدير بالذكر أن التقنيات الرقمية قد ساهمت في تعزيز كفاءة تقديم الخدمات الوطنية الحيوية، غير أن تزايد اعتماد الدولة على البنية التحتية للمعلومات الحيوية زاد من إمكانية تعرضها لمجموعة من المخاطر الجديدة. وقد تشمل تلك المخاطر تهديدات طبيعية أو من صنع الإنسان، متعمدة أو عرضية، من شأنها التأثير في سرية المعلومات التي تعتمد عليها الجهات الحكومية والمواطنون وقطاعات الأعمال ومستوى سلامتها ومدى توافرها.

تُعد سياسة حماية البنية التحتية للمعلومات الحيوية ركيزة محورية ولكنها في نفس الوقت تواجه عدة تحديات كامنة. حيث أدى التوسع في التقارب التقني إلى زيادة تعقيد منظومة ترابط تكنولوجيا الاتصالات والمعلومات داخل كل قطاع من جهة وبين القطاعات من جهة أخرى. ويؤدي هذا التعقيد إلى كثرة الجهات المعنية واتساع نطاق الإدارة. كما تفرض الخصائص الفريدة لكل قطاع أنواعاً مختلفة من الأصول والتهديدات والثغرات الأمنية التي تستلزم استحداث منهج إدارة خاص بكل قطاع. وستقوم الهيئة الوطنية للأمن الإلكتروني بإيجاد المنهج المناسب والتعاون الفعال بين الجهات المعنية ذات الصلة لمساعدتهم في الأنشطة الخاصة بهم في هذا الشأن.

١,٣
نطاق تطبيق السياسة

تسري السياسة على جميع البنى التحتية للمعلومات والجهات المنظمة والمُشغلة ذات الصلة والجهات المعنية المشاركة التي تدعم الخدمات الوطنية الحيوية في القطاعات الرئيسية والفرعية التالية، إضافةً إلى أي قطاعات أخرى قد تحددها الهيئة:

القطاعات الرئيسية	أهم القطاعات الفرعية
الصناعات الكيميائية	الصناعات الكيميائية الأساسية الصناعات الكيميائية المتخصصة
خدمات الطوارئ	خدمات الطوارئ أو الإنقاذ إنفاذ القانون
الصحة	الخدمات الطبية المختبرات
الطاقة النووية	المفاعلات النووية المواد النفايات
الإدارة العامة	الإدارة العامة الوطنية الإدارة العامة على صعيد الإمارة التعليم والبحث

القطاعات الرئيسية	أهم القطاعات الفرعية
المياه والكهرباء	التوليد النقل التوزيع إمداد المياه العام الصرف الصحي العام
الخدمات المالية	الخدمات المصرفية التأمين الأسواق المالية الاستثمارات
تكنولوجيا الاتصالات والمعلومات	نظم المعلومات الاتصالات السلكية واللاسلكية اتصالات الأقمار الاصطناعية وسائل الإعلام والبث الإذاعي
النفط والغاز	عمليات التنقيب واستخراج وإنتاج النفط الخام والغاز الطبيعي عمليات تكرير ومعالجة ونقل وبيع وتوزيع النفط الخام والغاز الطبيعي ومشتقاتهما
النقل	النقل البري النقل الجوي النقل البحري الخدمات اللوجستية والتخزين

الفصل الثاني

عملية حماية البنية التحتية للمعلومات الحيوية

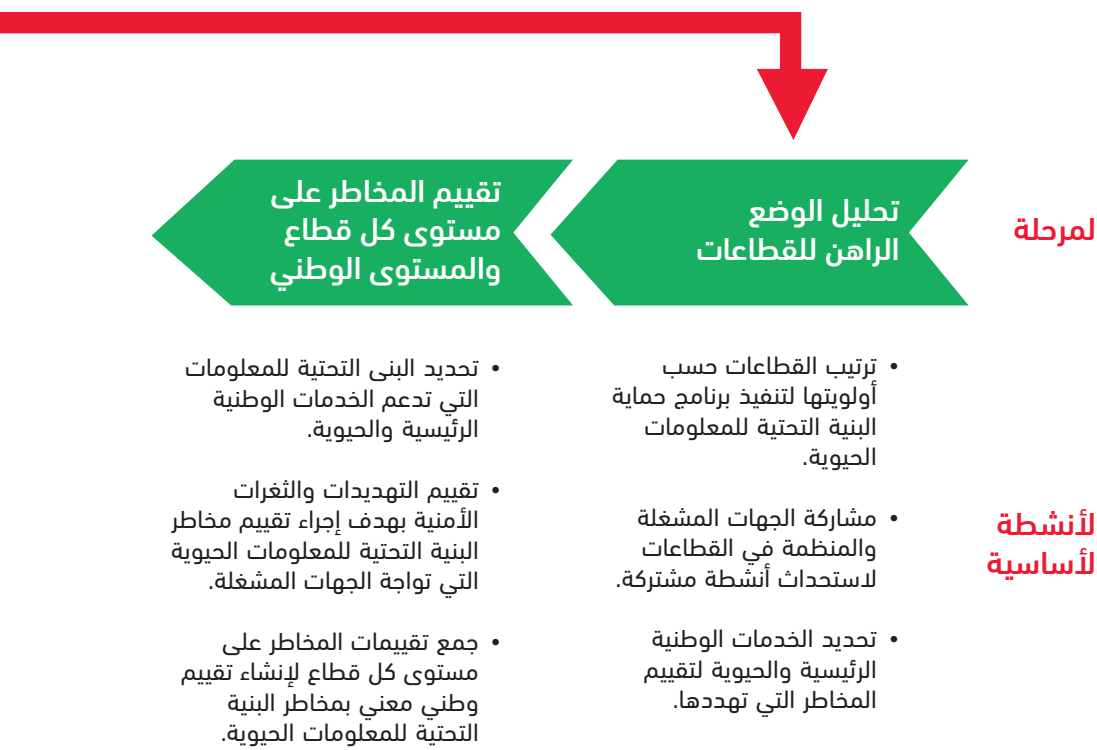
٢,٠

عملية حماية البنية التحتية للمعلومات الحيوية

تمثل عملية تحديد وتقييم وحماية البنية التحتية للمعلومات الحيوية على مستوى القطاع المحور الأساسي لبرنامج حماية البنية التحتية للمعلومات الحيوية لدولة الإمارات. كما تركز هذه العملية على ضمان التعاون بين الجهات المُنظمة والمُشغلة للبنية التحتية للمعلومات الحيوية وغيرها من الجهات المعنية المشاركة، إضافةً إلى متابعة تقدم وأداء البرنامج بأكمله.

وتتألف هذه العملية من أربع مراحل كما هو موضح في الشكل التالي:

الشكل التوضيحي(١): مراحل عملية حماية البنية التحتية للمعلومات الحيوية لدولة الإمارات



ينبغي تكرار العملية بأكملها بشكل دوري أو كلّما ارتأت الهيئة الوطنية للأمن الإلكتروني ضرورة ذلك (في حالة حدوث تغيير مهم مثلاً) في أي قطاع رئيسي ضمن نطاق برنامج الحماية.

وضع خطط القطاعات

- تحديد متطلبات الأمن الإلكتروني للبنية التحتية للمعلومات الحيوية التي ستساهم في الحد من المخاطر التي يتم اكتشافها.
- وضع خطط الحماية اللازمة لكل قطاع لتلبية متطلبات الأمن الإلكتروني للبنية التحتية للمعلومات الحيوية.

مراقبة تنفيذ خطط القطاعات

- تنفيذ خطط الحماية الموضوعة لكل قطاع.
- مراقبة تنفيذ الخطط لضمان تلبية المتطلبات الموضوعة.

تشمل كل مرحلة من مراحل العملية المذكورة أعلاه خطوات متعددة تستلزم تنفيذ أنشطة خاصة ومشاركة جهات معنية ذات الصلة. ويصف هذا المستند كلاً من الأنشطة المنفذة في كل خطوة إلى جانب المهام والمسؤوليات العامة لتلك الجهات المعنية.

٢,١
تحليل الوضع الراهن للقطاعات

تهدف هذه المرحلة إلى ترتيب خطوات تنفيذ سياسة الحماية حسب الأولوية على مستوى القطاعات الرئيسية، وتحديد الجهات المُنظمة (أو الجهة الرائدة في القطاع) والجهات المُشغلة والجهات المعنية وذات الصلة المطلوب مشاركتها في كل قطاع.

٢,١,١ ترتيب القطاعات حسب أولويتها لتنفيذ برنامج الحماية

تتولى الهيئة الوطنية للأمن الإلكتروني مسؤولية تنفيذ برنامج الحماية بشكل تدريجي على مستوى القطاعات العشرة الرئيسية المندرجة ضمن نطاق البرنامج، وستعمل على ترتيب تلك القطاعات حسب أولويتها لتنفيذ البرنامج من أجل تيسير توسيع نطاقه، استناداً إلى بعض العوامل التي تشمل على سبيل المثال لا الحصر ما يلي:

- الأهمية السياسية والاقتصادية والاجتماعية للقطاع.
- مستوى النضج المتوقع للأمن الإلكتروني في القطاع.
- مستويات الأنشطة الحالية للجهات المُشغلة ذات الصلة.
- المستوى الحالي لمخاطر التهديدات الإلكترونية على القطاع.
- عوامل أخرى تحددها الهيئة والجهات المعنية ذات الصلة.

٢,١,٢ مشاركة الجهات المعنية

تقوم الهيئة الوطنية للأمن الإلكتروني باختيار وإشراك الجهة المُنظمة والجهة المُشغلة والجهات المعنية المشاركة ذات الصلة في كل قطاع رئيسي بالاستعانة بفرق عمل لحماية البنية التحتية للمعلومات الحيوية الخاصة بالقطاعات، بهدف تعزيز أوجه التعاون من خلال الحوار والتنسيق المبكرين سعياً لتنفيذ أنشطة عملية الحماية بكفاءة وفعالية تامة.

وعلى صعيد آخر، ستتعاون الهيئة مع الجهة المُنظمة في كل قطاع رئيسي. وفي بعض الحالات (مثل عدم توافر جهة منظمة محددة), يمكن للهيئة الوطنية للأمن الإلكتروني أن تستعين بجهة أو جهات أخرى للقيام ببعض المسؤوليات والمهام التي عادة ما يتم منحها للجهة المُنظِمة للقطاع فيما يخص وضع ومتابعة تنفيذ برنامج حماية البنية التحتية للمعلومات الحيوية.

وفي المرحلة التالية، تقوم الهيئة، بالتعاون مع الجهة المُنظِمة للقطاع، بحصر أو تحديث الجهات المُشغلة والجهات المعنية ذات الصلة في كل قطاع حيوي لإشراكها في فرق العمل الخاصة بالقطاعات. ويحدد نموذج حوكمة حماية البنية التحتية للمعلومات الحيوية لدولة الإمارات الهيكل التنظيمي والتفويض المخول لفرق العمل الخاصة بالقطاعات والآلية التي ستعتمدها الهيئة الوطنية للأمن الإلكتروني والجهات المُنظِمة لتحديد أعضاء الفرق.

٢,١,٣ تحديد الخدمات الوطنية الحيوية

تقوم الهيئة الوطنية للأمن الإلكتروني بحصر الخدمات الوطنية الحيوية في كل قطاع حيوي، وذلك بالتعاون مع الجهات المُنظمة والمُشغلة.

لتحقيق هذه الغاية، يقوم فريق العمل المعني بكل قطاع بإعداد قائمة بالخدمات التي يدعمها على المستوى الوطني. وينصّ الإطار الوطني لإدارة المخاطر على المعايير التي ستطبقها كل القطاعات لتقييم أثر تعطل تلك الخدمات على المستوى الوطني ومؤشرات مستوى الخدمة الوطنية الحيوية. وبناء عليه ستقوم الهيئة الوطنية للأمن الإلكتروني بالحفاظ على القائمة الموحدة للخدمات الوطنية الحيوية للدولة على مستوى جميع القطاعات وتحديثها كلّما استلزم الأمر.

٢,٢

تقييم المخاطر على مستوى القطاع وعلى المستوى الوطني

يهدف هذا التقييم إلى اكتشاف وتحليل التهديدات والعواقب والثغرات الأمنية التي تتعرض لها الخدمات الوطنية الحيوية، ووفقاً لذلك يتم ترتيب الأولويات في تخصيص الموارد اللازمة. وينصّ الإطار الوطني لإدارة المخاطر لدولة الإمارات على عملية تحديد البنية التحتية للمعلومات الحيوية، والجهات المالكة أو المُشغلة ومستويات المخاطر، باستخدام منهج مبني على أهمية الخدمات.

الشكل التوضيحي(٢): مراحل عملية حماية البنية التحتية للمعلومات الحيوية

٢,٢,١ تحديد البنية التحتية للمعلومات الحيوية الداعمة للخدمات الوطنية

تقوم فرق العمل الخاصة بالقطاعات بتحديد أصول البنية التحتية للمعلومات التي تدعم تقديم الخدمات الوطنية الأساسية، وحصر عناصر تلك البنية التي قد تؤثر سلباً في الخدمات الوطنية في حالة توقفها أو تعرضها للخطر أو اختراقها أمنياً. ويتم اعتبار تلك الأصول جزءاً من البنية التحتية للمعلومات الحيوية على المستوى الوطني، كما سيتم تحديد الجهات المالكة أو المُشغلة للبنية التحتية للمعلومات الحيوية.

وستقوم الهيئة الوطنية للأمن الإلكتروني بتبني القائمة الختامية التي تضم البنية التحتية للمعلومات الحيوية والجهات المُشغلة لها.

٢,٢,٢ تقييم التهديدات والثغرات الأمنية

ينصّ الإطار الوطني لتقييم المخاطر الإلكترونية لدولة الإمارات على الخطوات التالية التي ينبغي على الجهات المُشغِلة للبنية التحتية للمعلومات الحيوية تنفيذها لكل بنية تقع تحت إدارتها:

تقييم التهديدات

تحديد الأسباب المحتملة للحوادث غير المرغوبة التي قد تُلحق الضرر بالبنية التحتية للمعلومات الحيوية.

تقييم الثغرات الأمنية

تقييم نقاط الضعف في البنية التحتية للمعلومات الحيوية التي يمكن استغلالها من قبل تهديد واحد أو أكثر، واحتمالية وقوع ذلك في ظل الضوابط الأمنية المطبقة.

جمع النتائج

دمج النتائج المستخلصة من تقييمي التهديدات والثغرات الأمنية مع تحليل الآثار المترتبة على الخدمات كما هو معرف في الإطار الوطني لتقييم المخاطر الإلكترونية، لتطوير تقييم لمخاطر الأمن الإلكتروني التي تواجه الجهة المُشغلة لبنية تحتية معينة.

تقوم الهيئة الوطنية للأمن الإلكتروني بالتعاون مع الجهة المنظمة للقطاع بتقديم المشورة والدعم للجهات المُشغلة للبنى التحتية للمعلومات الحيوية وللجهات المعنية ذات الصلة لمساعدتها على إجراء تقييم التهديدات والثغرات الأمنية، وإعداد تقييم مخاطر البنية التحتية للمعلومات الحيوية الخاص بالجهات المُشغلة التي ترفعها فيما بعد للجهة المُنظمة للقطاع.

٢,٢,٣ تقييم مخاطر الأمن الإلكتروني على مستوى القطاعات وعلى المستوى الوطني

تعمل كل جهة مُنظمة لقطاع من القطاعات (أو الجهة المُعينة / الجهة الرائدة في القطاع) على جمع تقييمات مخاطر البنية التحتية للمعلومات الحيوية الصادرة عن الجهات المُشغلة داخل قطاعها لاستحداث تقييم موحد لتلك المخاطر على مستوى كل قطاع. وستقدم الهيئة الوطنية للأمن الإلكتروني المشورة والدعم المطلوبين للجهات المُنظمة للقطاعات لمساعدتها في تنفيذ هذا النشاط، وتعمل الأخيرة بدورها بالتعاون مع الهيئة على مراجعة التقييم الموحد لاكتشاف أعلى مستويات المخاطر داخل كل قطاع، وأبرز المخاطر التي قد تنشأ داخل كل جهة مُشغلة بمفردها.

كما تقوم الهيئة الوطنية للأمن الإلكتروني بجمع تقييمات المخاطر لكل هذه القطاعات لإعداد تقييم موحد على المستوى الوطني من أجل اكتشاف أعلى مستويات المخاطر على صعيد جميع القطاعات، موفرة بذلك أساساً يمكن الاعتماد عليه لترتيب أولويات الموارد على النحو الذي يصبّ في مصلحة الأمن القومي لدولة الإمارات.

٢,٣
وضع خطط القطاعات

تنصّ الخطط الموضوعة للقطاعات على الإجراءات اللازمة لمواجهة أعلى مستويات المخاطر الواردة في تقييمات المخاطر على مستوى كل قطاع وعلى المستوى الوطني.

٢,٣,١ وضع متطلبات الأمن الإلكتروني للبنية التحتية للمعلومات الحيوية

تضع الهيئة الوطنية للأمن الإلكتروني بالتعاون مع الجهات المُنظِمة للقطاعات والجهات المشغلة للبنى التحتية للمعلومات الحيوية، متطلبات إلزامية لرفع مستوى الأمن الإلكتروني الخاص بالبنية التحتية للمعلومات الحيوية لتطبقها الجهات المُشغلة في كل قطاع، وللحد من المخاطر الواردة في تقييم المخاطر على مستوى كل قطاع وعلى المستوى الوطني ككل. وقد تشمل تلك المتطلبات المعايير الوطنية الخاصة بالقطاع التي تسري على جميع الجهات المُشغلة للبنى التحتية للمعلومات الحيوية في هذا القطاع، إضافةً إلى المتطلبات الخاصة بالجهات والمصممة خصيصاً لجهة مُشغلة بعينها.

٢,٣,٢ وضع خطط حماية للقطاعات

تقوم الجهة المُنظمة (بالتعاون مع الهيئة الوطنية للأمن الإلكتروني والجهات المُشغلة للبنية التحتية للمعلومات الحيوية ذات الصلة) بإعداد خطة لكل قطاع من القطاعات العشرة الرئيسية، بحيث تحدد الأنشطة الرئيسية والجهات المسؤولة عنها والجداول الزمنية اللازمة لتلبية متطلبات الأمن الإلكتروني للبنية التحتية للمعلومات الحيوية المحددة لذلك القطاع. وستكون الأنشطة الواردة في خطط القطاع موجهة نحو الجهات المُشغلة للبنية التحتية للمعلومات الحيوية ونحو جهات إضافية يتم تحديدها.

وستراجع الهيئة الوطنية للأمن الإلكتروني الخطط الموضوعة للقطاعات وتعتمدها قبل الشروع رسمياً في تنفيذها، وتعمل على ضمان التنسيق والملاءمة بين الخطط المقررة لمختلف القطاعات على المستوى الوطني.

ستُطلع الجهات المُشغلة لتلك البنى التحتية الجهة المُنظمة (والهيئة الوطنية للأمن الإلكتروني إذا اقتضت الحال ذلك) على خططها المقررة لتلبية المتطلبات السارية ضمن الإطار الزمني الخاص بخطط القطاعات. من ناحية أخرى، ستعتمد الهيئة خطط الجهات المُشغلة لتلبية متطلبات خطط القطاعات.

٢,٤
مراقبة تنفيذ خطط القطاعات

تُشرف الهيئة الوطنية للأمن الإلكتروني، بالتعاون مع الجهات المُنظمة للقطاعات (أو الجهة المُعينة/الجهة الرائدة في القطاع)، على تنفيذ خطط القطاعات ضماناً لوفاء الجهات المُشغلة بكافة المتطلبات الوطنية للأمن الإلكتروني الخاصة بالبنية التحتية للمعلومات الحيوية التي تنطبق عليها.

٢,٤,١ تنفيذ خطط القطاعات

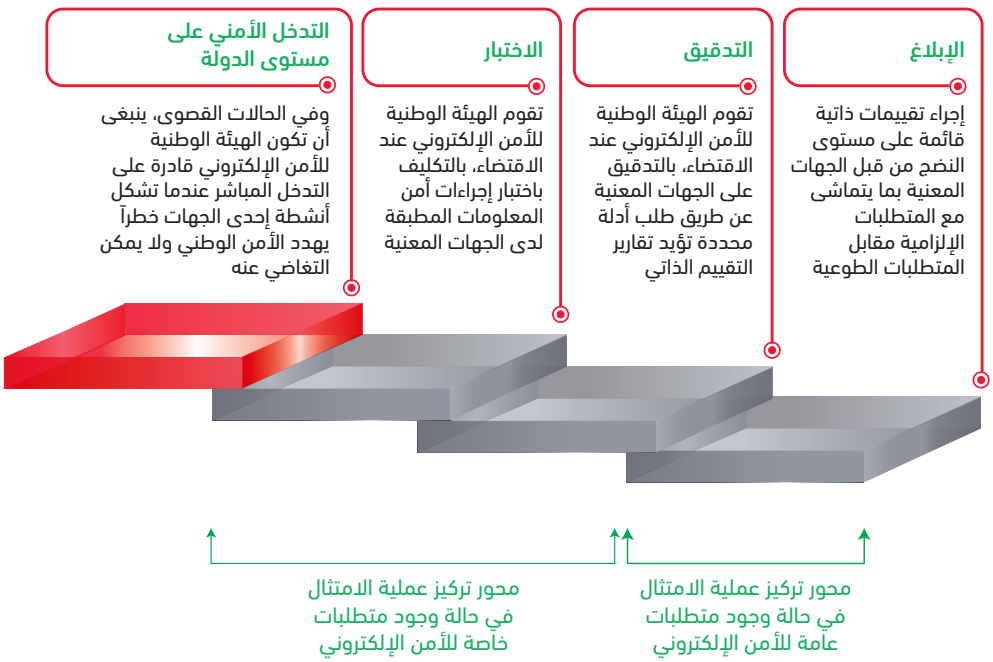
تلتزم كل جهة مُشغلة لتلك البنى التحتية بتلبية المتطلبات الواردة ضمن خطط القطاعات من خلال تنفيذ الخطط المعتمدة.

٢,٤,٢ مراقبة عملية التنفيذ

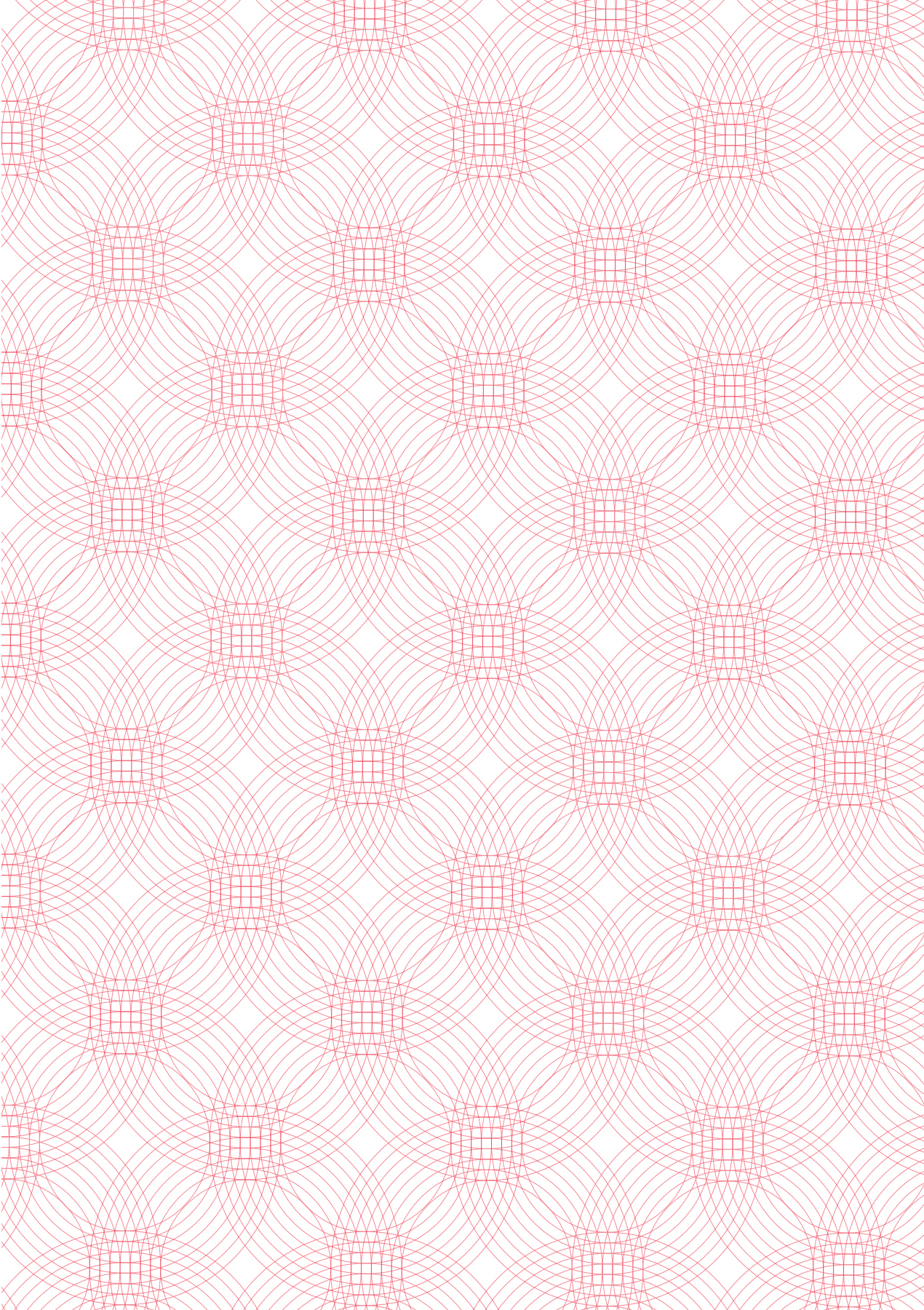
تتحقق الهيئة بشكل منتظم، بالتعاون مع الجهات المُنظمة، من قيام الجهات المُشغلة للبنية التحتية للمعلومات الحيوية بتنفيذ متطلبات خطط القطاعات. ولتيسير هذا الأمر، ستعمل كل جهة مُشغلة لتلك البنى التحتية على إطلاع الجهة المُنظمة المعنية والهيئة الوطنية للأمن الإلكتروني على التقدم المحرز في التنفيذ بشكل دوري. وستنصّ خطط القطاعات على توقيت إعداد التقارير التي ترفعها الجهات المُشغلة وعلى محتواها. وتقوم كل جهة مُنظمة بجمع التقارير الواردة من كل جهة مُشغلة في تقرير سير عمل معني بحماية البنية التحتية للمعلومات الحيوية على مستوى القطاع، ويتم رفعه إلى الهيئة الوطنية للأمن الإلكتروني.

وتقوم الهيئة من خلال نموذج حوكمة حماية البنية التحتية للمعلومات الحيوية لدولة الإمارات بتوضيح تفاصيل كلٍ من المستويات الأربعة التي ستستخدمها الهيئة الوطنية للأمن الإلكتروني في مراقبة أداء الجهات المُشغلة في تنفيذ جميع جوانب الخطط الموضوعة للقطاعات.

الشكل التوضيحي (٣): تصعيد عملية الامتثال للضوابط الأمنية



كما ستقوم الهيئة من خلال نموذج حوكمة حماية البنية التحتية للمعلومات الحيوية بوضع آلية تصعيد مستوى مراقبة التنفيذ ضمن جهة مُشغلة لتلك البنى التحتية أو قطاع بعينه.



الفصل الثالث

مراقبة برنامج الإمارات لحماية البنية التحتية للمعلومات الحيوية

٣,٠
مراقبة برنامج الإمارات لحماية البنية التحتية للمعلومات الحيوية

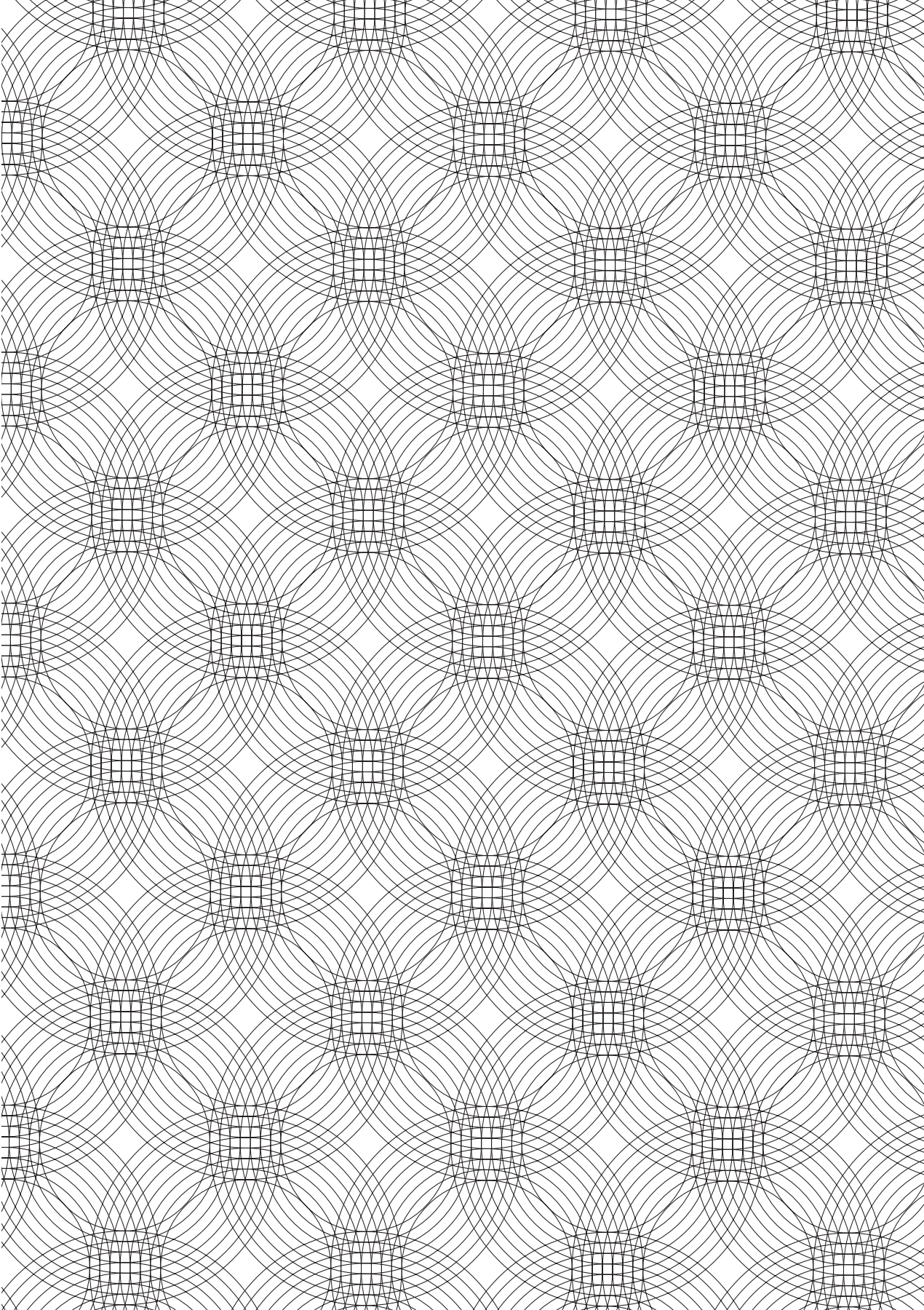
تزامناً مع مراقبة تنفيذ خطط القطاعات، ستعمل الهيئة الوطنية للأمن الإلكتروني أيضاً على متابعة برنامج حماية البنية التحتية للمعلومات الحيوية بالتعاون مع الجهات المنظمة للقطاعات، من أجل قياس النتائج وتحديد المشكلات المحتملة وتعزيز إجراءات التحسين. وستقوم الهيئة من خلال نموذج حوكمة حماية البنية التحتية للمعلومات الحيوية وبالتعاون مع الجهات المعنية بوضع مجموعة من المقاييس لقياس ثلاثة جوانب رئيسية لبرنامج الحماية، وهي على النحو التالي:

التقدم المحرز على صعيد التنفيذ
يقيس التقدم المحرز في تنفيذ جميع مراحل عملية الحماية، كما يسلط الضوء على أوجه التباين مع الخطط الأصلية بهدف اتخاذ الإجراءات التصحيحية.

الفعالية
يقيس مدى فعالية برنامج الحماية في تطوير مستوى أمن البنية التحتية للمعلومات الحيوية على صعيد القطاع ودولة الإمارات.

الأثر
يقيس الأثر المترتب على الأعمال أو المهام والناجم عن تنفيذ برنامج الحماية.

ستعمل كل من الجهات المُنظمة والمُشغلة للبنية التحتية للمعلومات الحيوية على إمداد الهيئة الوطنية للأمن الإلكتروني بكل ما يلزمها من معلومات لتحديث تلك المقاييس.



الفصل الرابع

المنهج التعاوني لحماية البنية التحتية للمعلومات الحيوية

٤,٠
المنهج التعاوني لحماية البنية التحتية للمعلومات الحيوية

تعزز الهيئة الوطنية للأمن الإلكتروني من بيئة العمل التعاوني مع الجهات المُنظمة للقطاعات والجهات المُشغلة للبنية التحتية للمعلومات الحيوية وغيرها من الجهات المعنية ذات الصلة من أجل تسهيل التطبيق الناجح لبرنامج الحماية. وسينصبّ تركيز المنهج التعاوني المذكور على التحسينات الملموسة في إطار الحماية خلال فترة زمنية مناسبة. وستطلب الهيئة اتخاذ تدابير محددة عند الاقتضاء، سعياً للوصول إلى مستويات أكثر تقدماً من الأمن الإلكتروني للبنية التحتية للمعلومات الحيوية في دولة الإمارات.

وستقوم الهيئة من خلال نموذج حوكمة حماية البنية التحتية للمعلومات الحيوية بوضع الآلية التي ستتفاعل في إطارها جميع الجهات المعنية بحماية البنية التحتية للمعلومات الحيوية عبر فرق عمل وطنية وأخرى خاصة بالقطاعات تعنى بحماية البنية التحتية.

تعمل فرق العمل على مساعدة الهيئة الوطنية للأمن الإلكتروني والجهات المعنية ذات الصلة على مباشرة ما يلي:

- **وضع أنشطة التخطيط الخاصة بحماية البنية التحتية للمعلومات الحيوية الخاصة بالقطاع.**
- **تنفيذ الأنشطة الواردة ضمن مراحل عملية حماية البنية التحتية للمعلومات الحيوية.**
- **مراقبة تنفيذ عملية حماية البنية التحتية للمعلومات الحيوية داخل القطاعات الرئيسية، واقتراح إجراءات تصحيحية كلّما دعت الحاجة.**

تنصّ السياسة الوطنية لتبادل المعلومات على المتطلبات اللازمة للقدرات الوطنية (النظام الوطني) لتبادل المعلومات من أجل دعم أنشطة فرق العمل مع حماية الطبيعة الحساسة للمعلومات المتبادلة بين المتنافسين المحتملين.

الملاحق

الملحق ا

السياسات الداعمة لحماية البنية التحتية للمعلومات الحيوية

مكونات برنامج حماية البنية التحتية للمعلومات الحيوية	السياسة / الآلية الداعمة
عملية حماية البنية التحتية للمعلومات الحيوية	نموذج حوكمة حماية البنية التحتية للمعلومات الحيوية لدولة الإمارات. الإطار الوطني لإدارة المخاطر لدولة الإمارات العربية المتحدة.
مراقبة البرنامج	نموذج حوكمة حماية البنية التحتية للمعلومات الحيوية لدولة الإمارات.
التعاون على حماية البنية التحتية للمعلومات الحيوية وفرق العمل	نموذج حوكمة حماية البنية التحتية للمعلومات الحيوية لدولة الإمارات. السياسة الوطنية لتبادل المعلومات الخاصة بالأمن الإلكتروني.

الملحق ٢
التعريفات الرئيسية

المصطلح	التعريف
برنامج حماية البنية التحتية للمعلومات الحيوية	خطة وطنية تم تطويرها من قبل الهيئة الوطنية للأمن الإلكتروني تشمل المبادرات والأفعال الرئيسية لتعزيز الجاهزية والاستجابة للحوادث الإلكترونية التي تستهدف أمن البنية التحتية للمعلومات الحيوية.
البنية التحتية للمعلومات الحيوية	أصول المعلومات المادية والافتراضية التي تدعم تنفيذ وظيفة بالغة الأهمية وتقديم خدمة حيوية.
الجهة المُشغلة للبنية التحتية للمعلومات الحيوية	هي الجهة المسؤولة عن الاستثمارات القائمة في البنية التحتية للمعلومات الحيوية أو عمليات تشغيلها اليومية أو كلتاهما.
القطاع الحيوي	قطاع معروف على الصعيد الوطني بتوفير خدمة حيوية أو أكثر.
الوظائف الحيوية	مجموعة من العمليات الضرورية لإنتاج وتوفير والحفاظ على الخدمات والمنتجات الحيوية.
الخدمة الحيوية	خدمة مهمة قد يكون لتعطيلها أو تدميرها أثر بالغ من الناحية الأمنية أو الاقتصادية أو الاجتماعية على دولة الإمارات.
أصول المعلومات	أصول مادية أو افتراضية لنظم تكنولوجيا المعلومات والاتصالات مثل البيانات والنظم والمنشآت والشبكات وأجهزة الكمبيوتر.
البنية التحتية للمعلومات	مجمل أصول المعلومات المادية والافتراضية التي تشكل جزءاً من بنية تحتية معينة.
النظام الوطني لمشاركة المعلومات (للأمن الإلكتروني)	مجموعة من السياسات والإجراءات والنظم وآليات العمل اللازمة لتبادل المعلومات المتعلقة بأمن المعلومات بطريقة فعالة وبناء على متطلبات محددة.
الجهة المنظمة	الهيئة الحكومية التي تضع اللوائح وتراقب امتثال وسلوك الجهات الخاضعة للتنظيم في قطاع معين (أو سوق).
خطط القطاعات	خطط مفصلة تضعها الجهات المنظمة للقطاعات التي يتم اعتمادها من قبل الهيئة الوطنية للأمن الإلكتروني تحدد الإجراءات والجهات المسؤولة والجداول الزمنية اللازمة للتصدي لأعلى مستويات المخاطر التي تم تحديدها في تقييمات المخاطر على الصعيد الوطني وصعيد كل هذه القطاعات، وتوجيه تطبيق متطلبات الأمن الإلكتروني والحماية للبنية التحتية للمعلومات الحيوية.

فريق العمل لحماية البنية التحتية للمعلومات الخاصة بالقطاع	فريق حوكمة خاصة بالقطاع تشترك الهيئة الوطنية للأمن الإلكتروني في رئاسته إلى جانب الجهة المنظمة للقطاع (أو جهة رائدة للقطاع أو ممثل عنه) ويتألف من الهيئة الوطنية للأمن الإلكتروني والجهة المنظمة للقطاع والجهات المشغلة وجهات معنية أخرى لتعزيز التعاون ودعم التخطيط داخل القطاع وتنفيذ الأنشطة ومراقبتها للرفع من حماية البنية التحتية للمعلومات الحيوية.
فريق العمل الوطني لحماية البنية التحتية للمعلومات	فريق حوكمة يشمل القطاعات، برئاسة الهيئة الوطنية للأمن الإلكتروني ويتألف من الهيئة الوطنية للأمن الإلكتروني والجهات المنظمة للقطاع (رواد القطاعات أو ممثلون عنهم) وجهات معنية أخرى لتعزيز التعاون داخل القطاع ودعم التخطيط على الصعيد الوطني وصعيد القطاعات وتنفيذ الأنشطة ومراقبتها للرفع من حماية البنية التحتية للمعلومات الحيوية.

[1] سيتم تبيان المعايير المفصلة التي تستخدم لتحديد الخدمة الحيوية في المرحلة الأولى من عملية سياسة الإمارات العربية المتحدة لحماية البنية التحتية للمعلومات الحيوية.