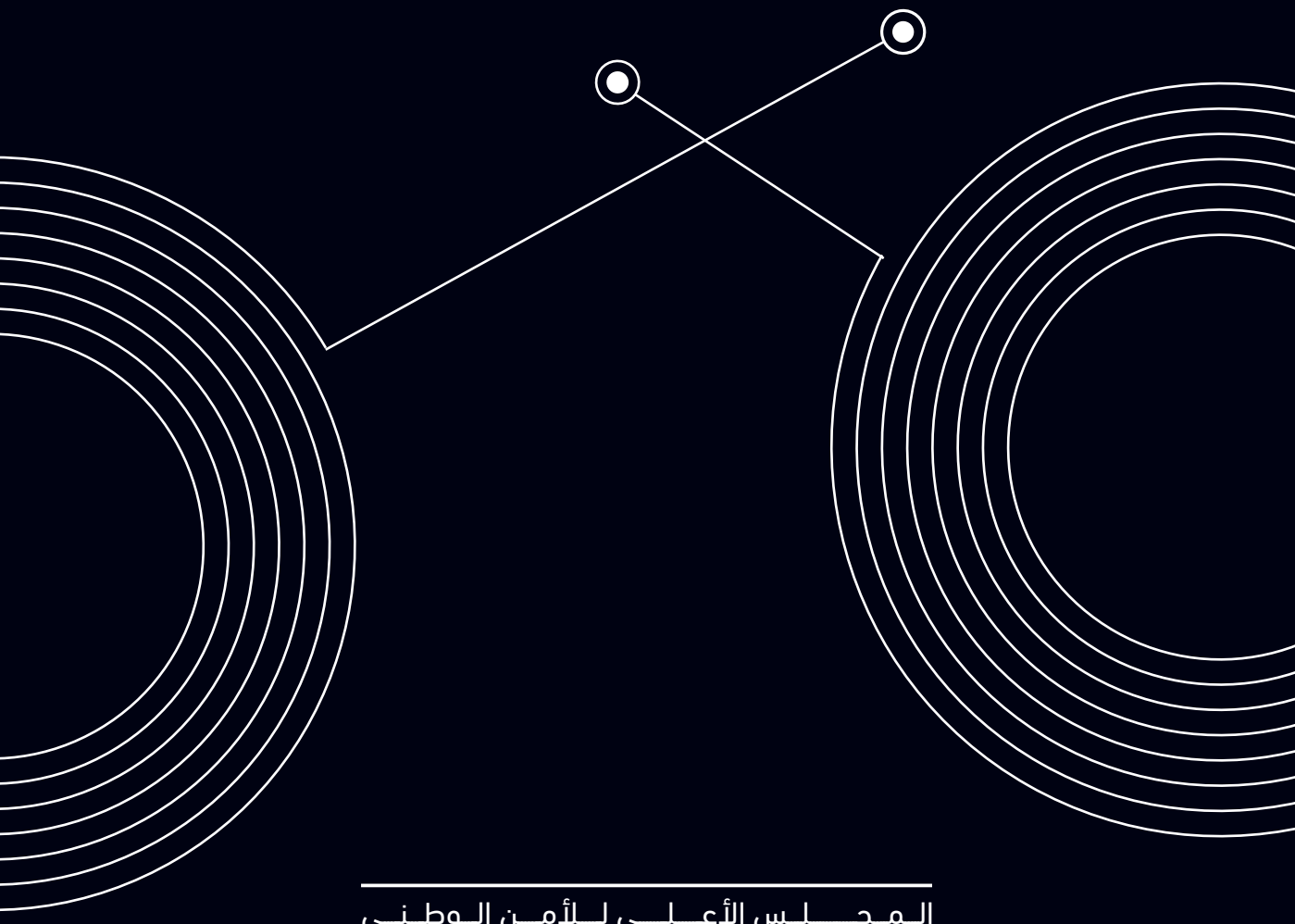
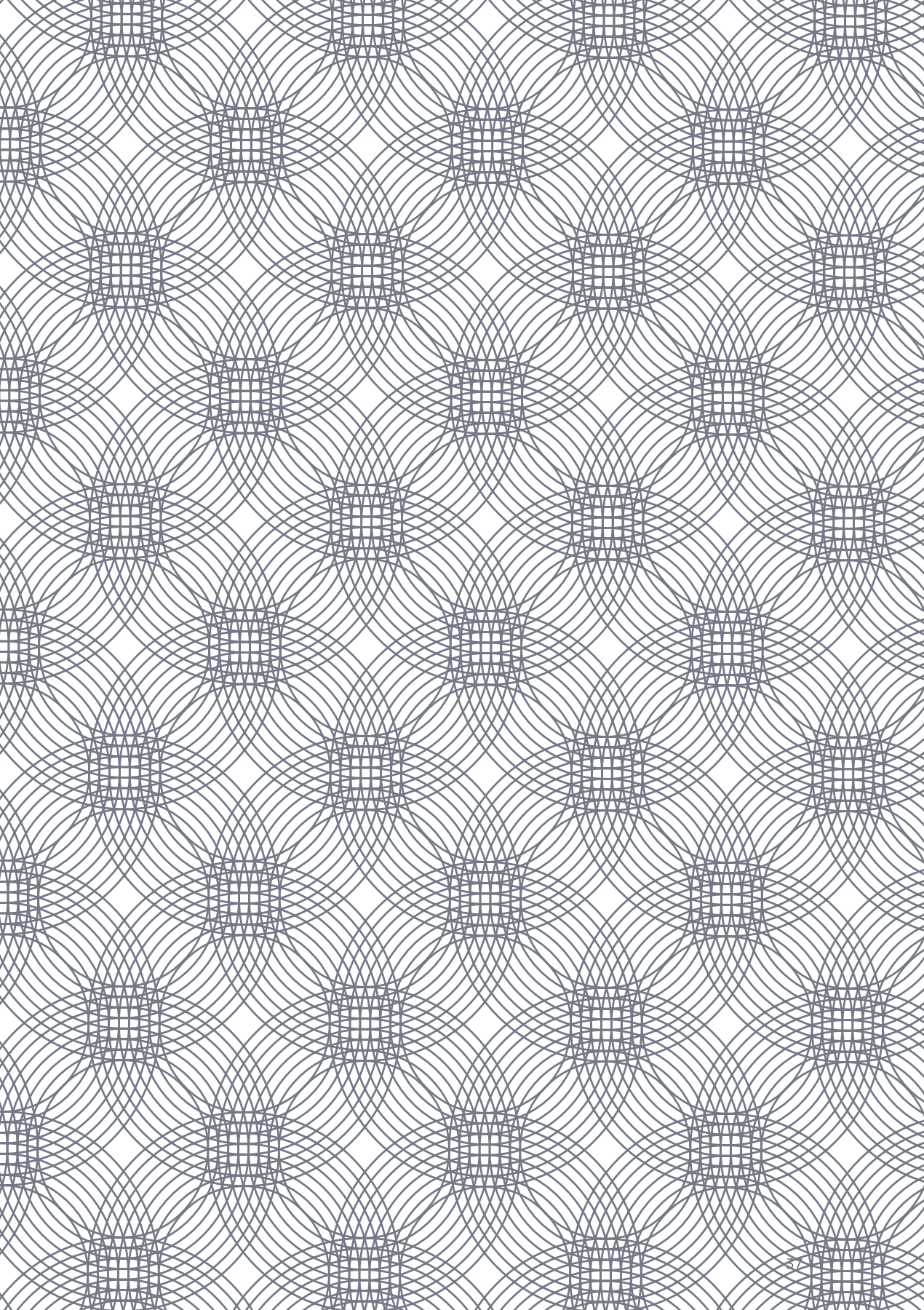
الهيئة الوطنية للأمن الإلكتروني
NATIONAL ELECTRONIC SECURITY AUTHORITY
UNITED ARAB EMIRATES الإمارات العربية المتحدة

الإطار الوطني لضمان أمن المعلومات



المجلس الأعلى للأمن الوطني

جدول المحتويات



تمهيد

سعياً منا لتحقيق رؤية الإمارات العربية المتحدة الرامية إلى تكوين 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 والاجراءات 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، والتي 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.

ويدعم الإطار الوطني لضمان المعلومات والوارد وصفه في هذا المستند، تنفيذ هذه الاستراتيجية. ويهدف إلى إطلاع الجهات المعنية على مكونات الإطار الوطني لضمان المعلومات الرامي إلى تحقيق هدفين جوهريين هما:

- الارتقاء بالحد الأدنى لمستويات الأمن الإلكتروني في جميع الجهات العاملة في الدولة من خلال مساعدتها على تشكيل فهم عام لمتطلبات ضمان أمن المعلومات على مستوى الجهات.
- الارتقاء بمستويات أمن البنية التحتية للمعلومات التي تدعم تقديم الخدمات الوطنية الأساسية عبر ربط الجهات مع بعضها بعضاً على مستوى قطاعات الأعمال وعلى مستوى الدولة.

تُصدر الهيئة الوطنية للأمن الإلكتروني الإطار الوطني لضمان المعلومات وتتولى مهمة إدارته، ويتم توجيه أي استفسار أو استيضاح أو اقتراح بشأن محتوى هذا المستند إلى الهيئة.

١,٢
مبادئ ضمان أمن المعلومات

يُعرف ضمان أمن المعلومات بأنه حماية المعلومات وإدارة المخاطر واستمرارية الأعمال المرتبطة باستخدام ومعالجة وتخزين ونقل المعلومات أو البيانات، والنظم والإجراءات المستخدمة لتلك الأغراض.

بينما يُركز ضمان أمن المعلومات في المقام الأول على المعلومات في شكلها الرقمي، فإن نطاقه الكامل يشمل أيضاً الأشكال المادية للمعلومات، بهدف حمايتها إلى أقصى حد ممكن بغض النظر عن شكلها وبطريقة تتناسب مع أهميتها وقيمتها.

ويعتبر أمن المعلومات جزءاً من مفهوم ضمان المعلومات الذي يشمل نطاقاً أعرض من مفاهيم حماية وإدارة المعلومات مثل إدارة استمرارية المعلومات، والتعافي من الكوارث، ومراقبة الامتثال، وإصدار الشهادات والاعتمادات وغيرها.

تتمثل المبادئ الخمسة الرئيسية لضمان المعلومات فيما يلي:

١,٢,١ السرية

يضمن مبدأ السرية حصر إمكانية النفاذ إلى المعلومات على الأشخاص المصرح لهم بالاطّلاع عليها، وحظر إتاحتها أو الإفصاح عنها إلى الجهات غير المصرح لها بذلك. ويتطلب هذا الأمر من المسؤولين عن حفظ المعلومات أو معالجتها أو نقلها اتخاذ الحيطة اللازمة لمكافحة الاختراقات الأمنية المتعمّدة أو العَرضية.

١,٢,٢ السلامة

يضمن مبدأ السلامة منع أي جهة من تغيير المعلومات دون اكتشاف ذلك.

١,٢,٣ التوفر

يضمن مبدأ التوفر سهولة النفاذ إلى أصول المعلومات واستخدامها عند الحاجة من قبل الجهة المصرح لها بذلك. وفي هذا السياق، تشمل أصول المعلومات البيانات والنظم والمنشآت والشبكات وأجهزة الحاسب الآلي.

١,٢,٤ التحقق من الهوية

يُعرف مبدأ التحقق من الهوية بأنه عملية تحديد ما إذا كان ادعاء الهوية الذي أدلت به جهة ما صحيح أم لا. تقدم الجهة بيانات اعتمادها أثناء عملية التحقق من الهوية وتتم المصادقة عليها من خلال مطابقتها ببيانات الاعتماد المخزنة في النظام.

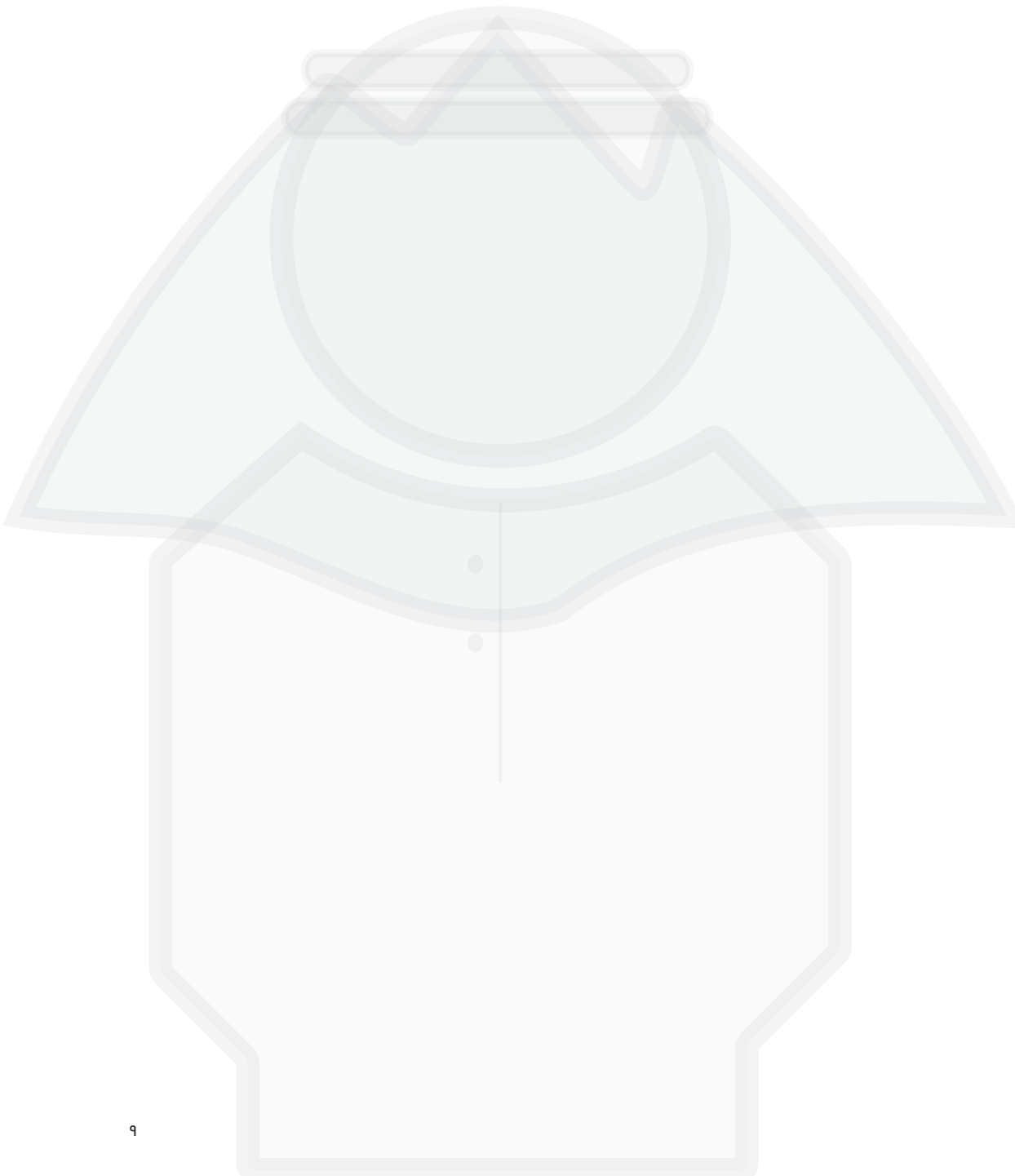
١,٢,٥ عدم الإنكار

يوفر مبدأ عدم الإنكار إثبات منشأ البيانات، حيث يضمن أن مرسل الرسالة لن ينكر إرساله لها في وقت لاحق وأن متلقي الرسالة لن ينكر استلامه لها.

١,٣
أطر ضمان أمن المعلومات الحالية

ثمة العديد من أطر عمل ضمان أمن المعلومات المتاحة لعامة الجهات، ولكن معظمها مُصمم لتنفيذه داخل جهة واحدة فحسب. وبينما تتضمن العديد من أطر العمل أحكاماً لتنظيم عملية الاتصال الشبكي المباشر بين جهات معينة (مثل المشتري والمورد)، إلا أن معظمها لا تأخذ في الحسبان مشكلات ضمان أمن المعلومات التي تنشأ من الترابط المنهجي بين المنظمات الحديثة على مستوى كافة القطاعات في الدولة.

فعلى سبيل المثال، تملك العديد من الجهات في الدولة قدرات وأطر داخلية لضمان المعلومات يعتمد تصميمها على مجموعة كبيرة من أفضل الممارسات المتبعة في هذا السياق، وتم العمل على تصميمها خصيصاً لتلبية احتياجات جهة ما، وغالباً ما تكون في سياق خاص. ولا يساهم هذا المنهج في تحقيق نفس النتائج المنشودة على مستوى جهات مختلفة، ولا في تكوين مجتمع لضمان المعلومات على مستوى قطاع محدد من قطاعات الأعمال المختلفة (بما فيها الإدارة العامة) أو على مستوى الدولة، تعمل في إطاره جميع الجهات سوياً لمواجهة التحديات المشتركة في مجال ضمان أمن المعلومات. وقد يؤدي هذا إلى تداخل الجهود وازدواجية القدرات التي تستنزف موارد نفيسة دون فائدة تُرجى، وربما قد يؤدي ذلك إلى ما هو أكثر خطورة وهو وجود ثغرات أمنية يتعذر على أي جهة أو مجموعة خاصة داخل إحدى الجهات، التصدي لها بمعزل عن الآخرين.

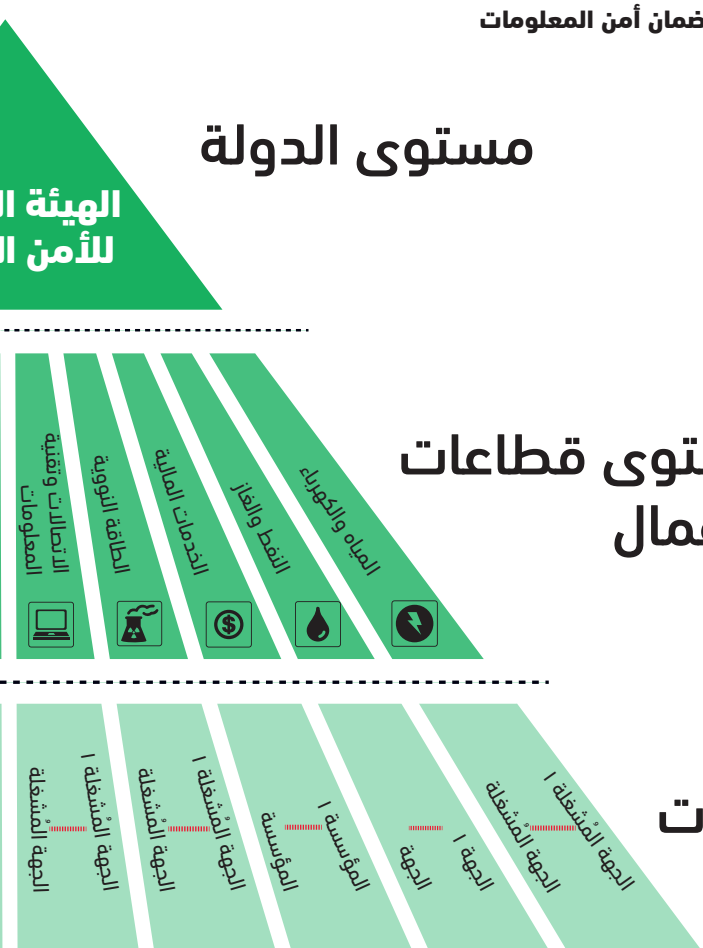


١,٤

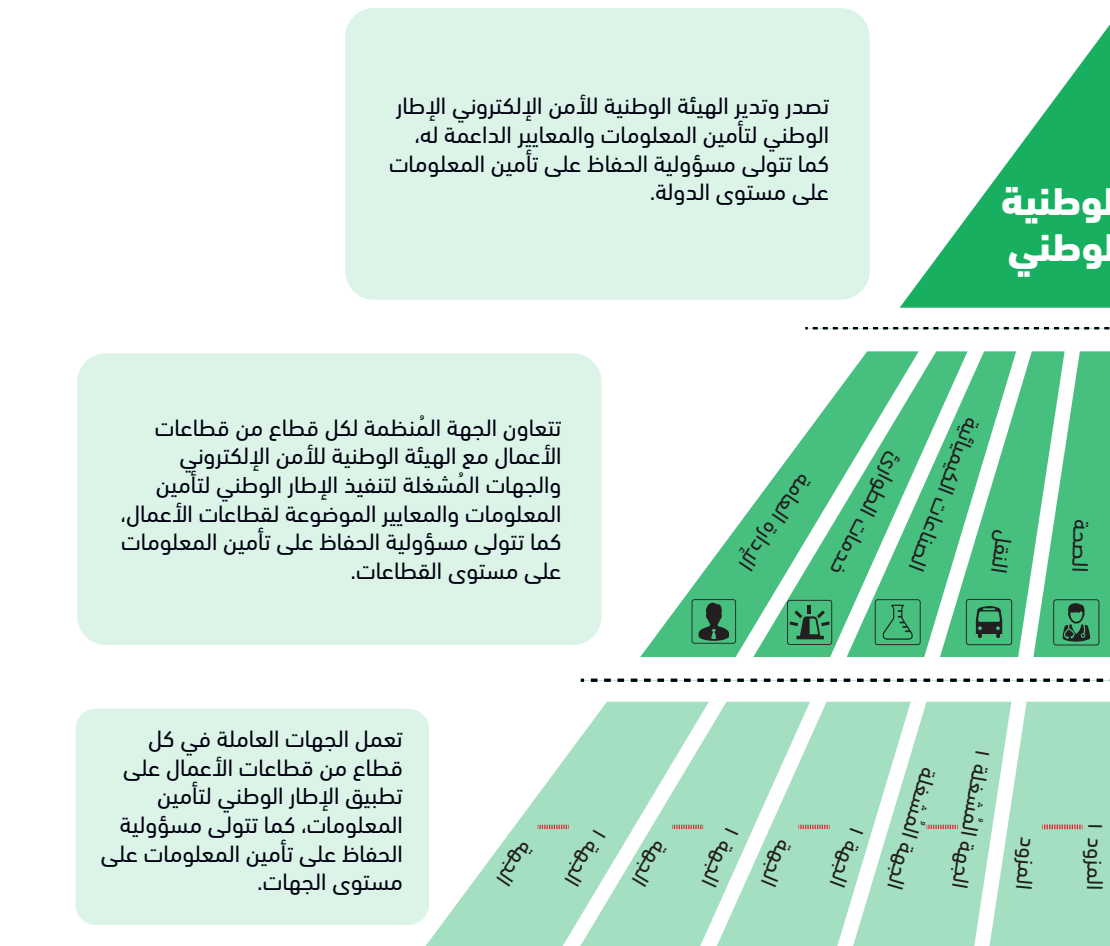
ضمان أمن المعلومات على مستوى القطاعات وعلى مستوى الدولة

من أجل المساعدة على تخطي تلك القيود، يتناول الإطار الوطني لضمان المعلومات لدولة الإمارات قضايا الأمن الإلكتروني على مستوى الجهات وقطاعات الأعمال والدولة. وليس الغرض من هذا استبدال أي إطار عمل قائم لضمان المعلومات داخل أي جهة أو مجموعة جهات معينة تعمل ضمن إطار مشترك، ولكن الغرض هو إنشاء نموذج مرجعي يمكن تطبيقه إضافةً إلى أي إطار عمل أو معايير داخلية لضمان المعلومات القائمة.

الشكل التوضيحي ١: مستويات تطبيق ضمان أمن المعلومات



يضع الإطار الوطني الحد الأدنى المطلوب من قدرات ضمان أمن المعلومات في جميع الجهات العاملة في الدولة، مع تحديد الآليات ذات القيمة المضافة لكل جهة للاندماج داخل سياق ضمان أمن المعلومات مع الجهات المعنية الأخرى على مستوى القطاعات وعلى مستوى الدولة.

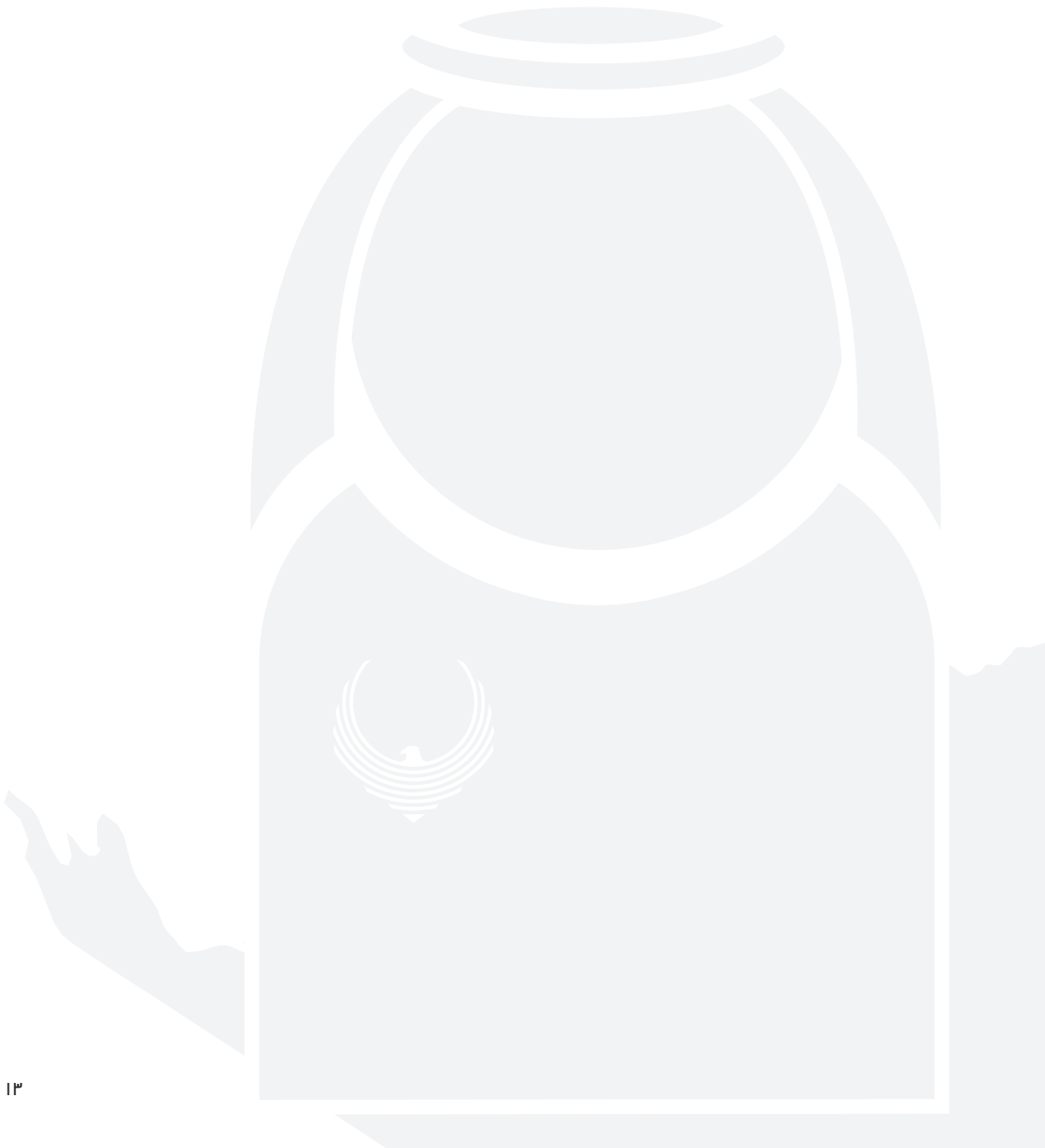


ويساهم الحد من الأطر المستقلة الناشئة عن تطبيق مناهج ضمان أمن المعلومات لكل جهة على الفاعلية في الحد من المخاطر الإلكترونية وازدواجية الجهود بين الجهات، ما يوجد سياقاً أكثر قوة وتكاملاً وكفاءة لضمان المعلومات على مستوى الدولة، ويتسم بجاهزية أكبر لحماية الدولة من التهديدات الإلكترونية.

١,٠
نطاق تطبيق الإطار الوطني لضمان أمن المعلومات

سيكون الامتثال للإطار الوطني لضمان المعلومات أمراً إلزامياً على جميع الجهات الحكومية وغيرها من الجهات التي ترى الهيئة الوطنية للأمن الإلكتروني أنها تحظى بأهمية بالغة [١] في قطاعات الأعمال الأخرى. فضلاً عن ذلك، تُوصي الهيئة جميع الجهات الأخرى العاملة في الدولة باتباع الإرشادات الأمنية بشكل طوعي سعياً للارتقاء بالحد الأدنى لمستويات الأمن على مستوى الدولة.

[١] تنصّ سياسة حماية البنية التحتية للمعلومات الحيوية لدولة الإمارات الصادرة عن الهيئة الوطنية للأمن الإلكتروني على القطاعات والجهات التي تُصنف على أنها "حيوية".



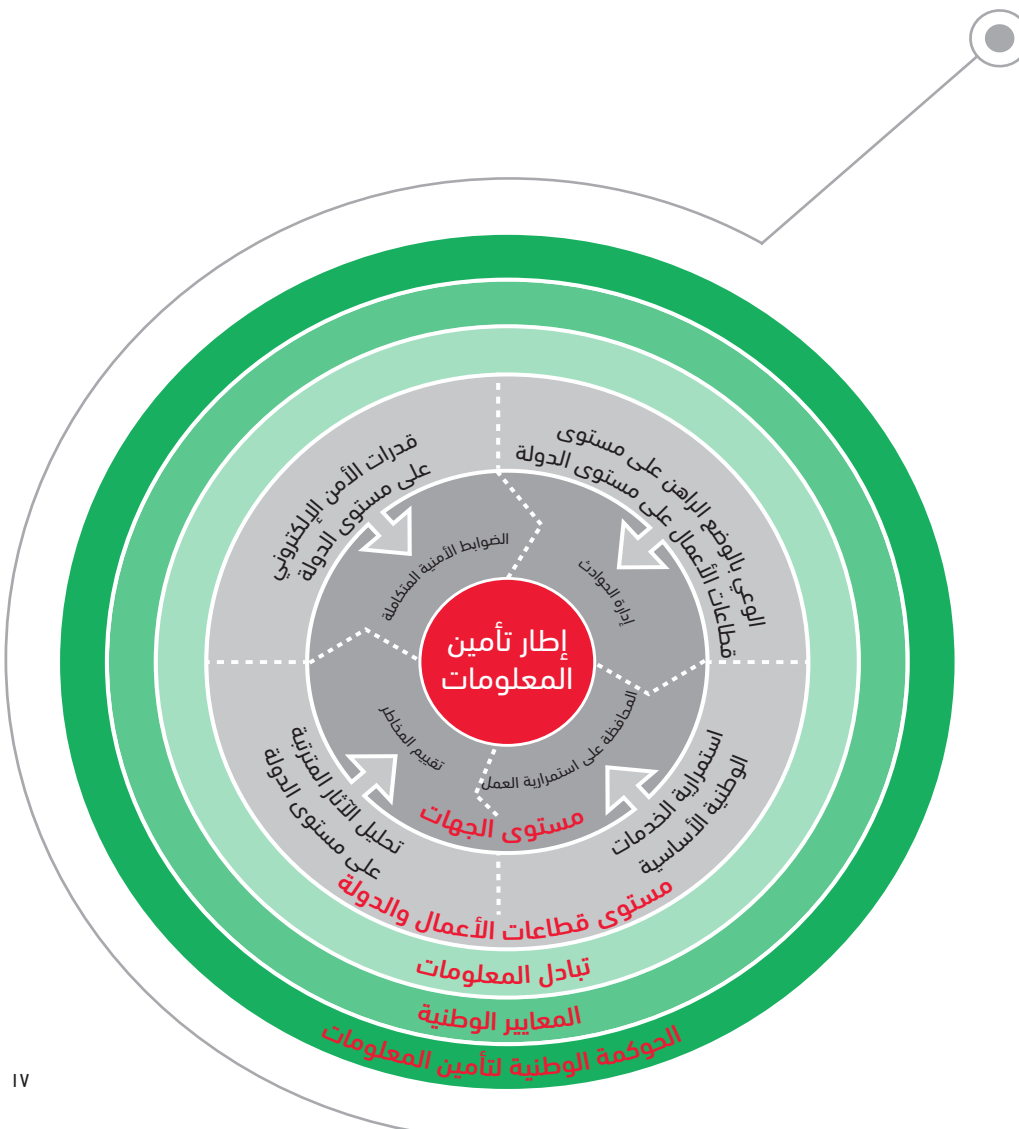
الفصل الثاني

الإطار الوطني لضمان أمن المعلومات للإمارات العربية المتحدة

٢,٠
الإطار الوطني لضمان أمن المعلومات للإمارات العربية المتحدة

يُحدد الإطار الوطني ضمان أمن المعلومات على مستوى الجهات وقطاعات الأعمال المختلفة (بما فيها القطاع الحكومي أو الإدارة العامة) والدولة استناداً إلى منهج قائم على دورة العمل المدعمة بمجموعة من المعايير الوطنية، والقدرات القوية لتبادل المعلومات، وبرنامج شامل للحوكمة تُديره الهيئة الوطنية للأمن الإلكتروني.

الشكل التوضيحي(٢): الإطار الوطني لضمان أمن المعلومات



ضمان المعلومات على مستوى الجهة

منهج قائم على المخاطر يسعى لتحديد أصول المعلومات الأساسية والعمل على حمايتها داخل كل جهة.

ضمان المعلومات على مستوى القطاعات والدولة

مكونات ذات قيمة مضافة تعمل على إنشاء روابط بين الجهات من ناحية وقطاعات الأعمال المختلفة (بما فيها الإدارة العامة) والدولة من ناحية أخرى.

تبادل المعلومات

الآلية الرئيسية التي تعمل بمقتضاها الجهات لتبادل المعلومات والبيانات مع الجهات الخارجية.

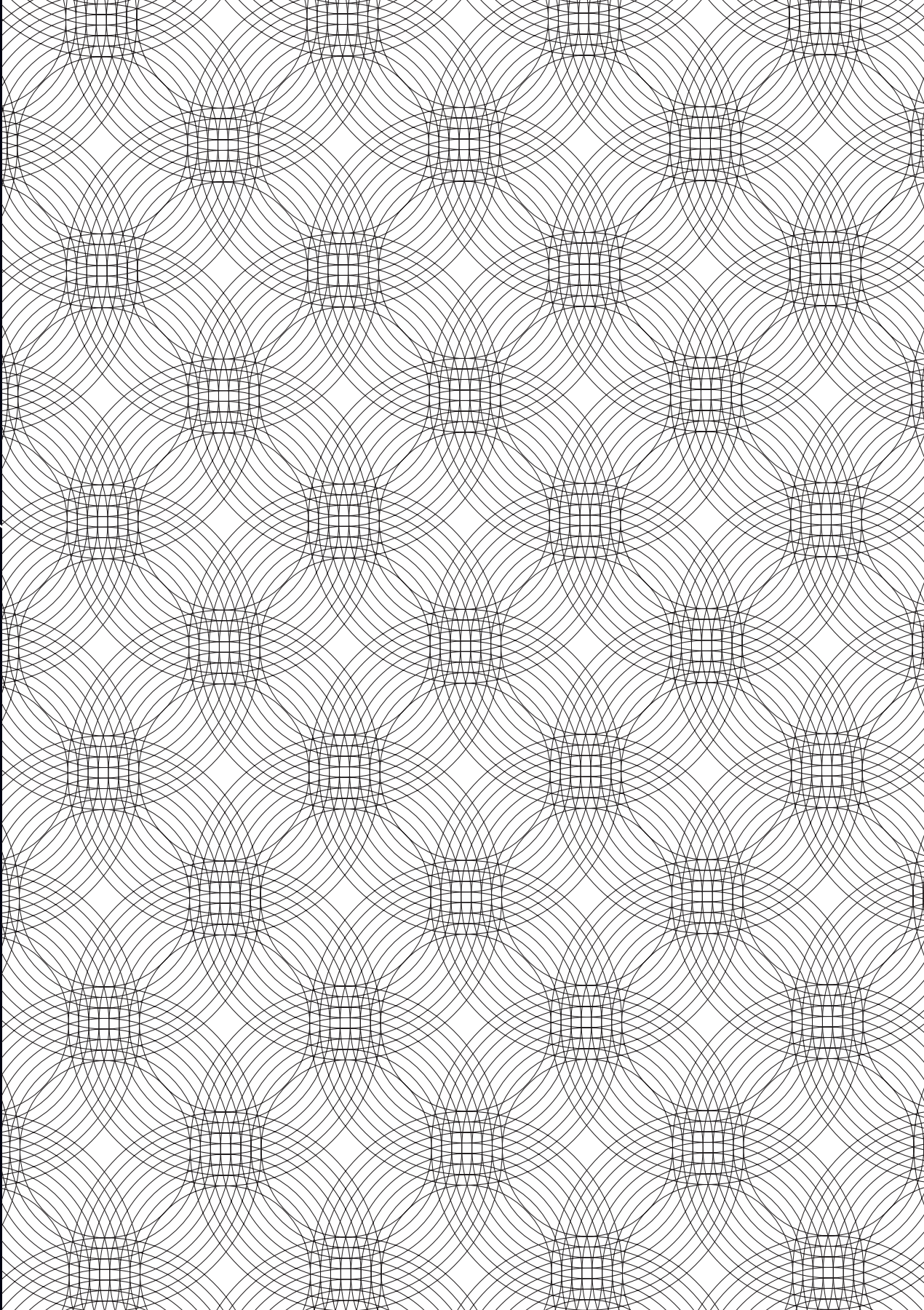
المعايير الوطنية لضمان المعلومات

المعايير العامة والخاصة بكل قطاع والخاصة للمنتجات أو الخدمات، او التي تطبق على الجهات المختلفة والمعنية.

حوكمة ضمان أمن المعلومات على مستوى الدولة

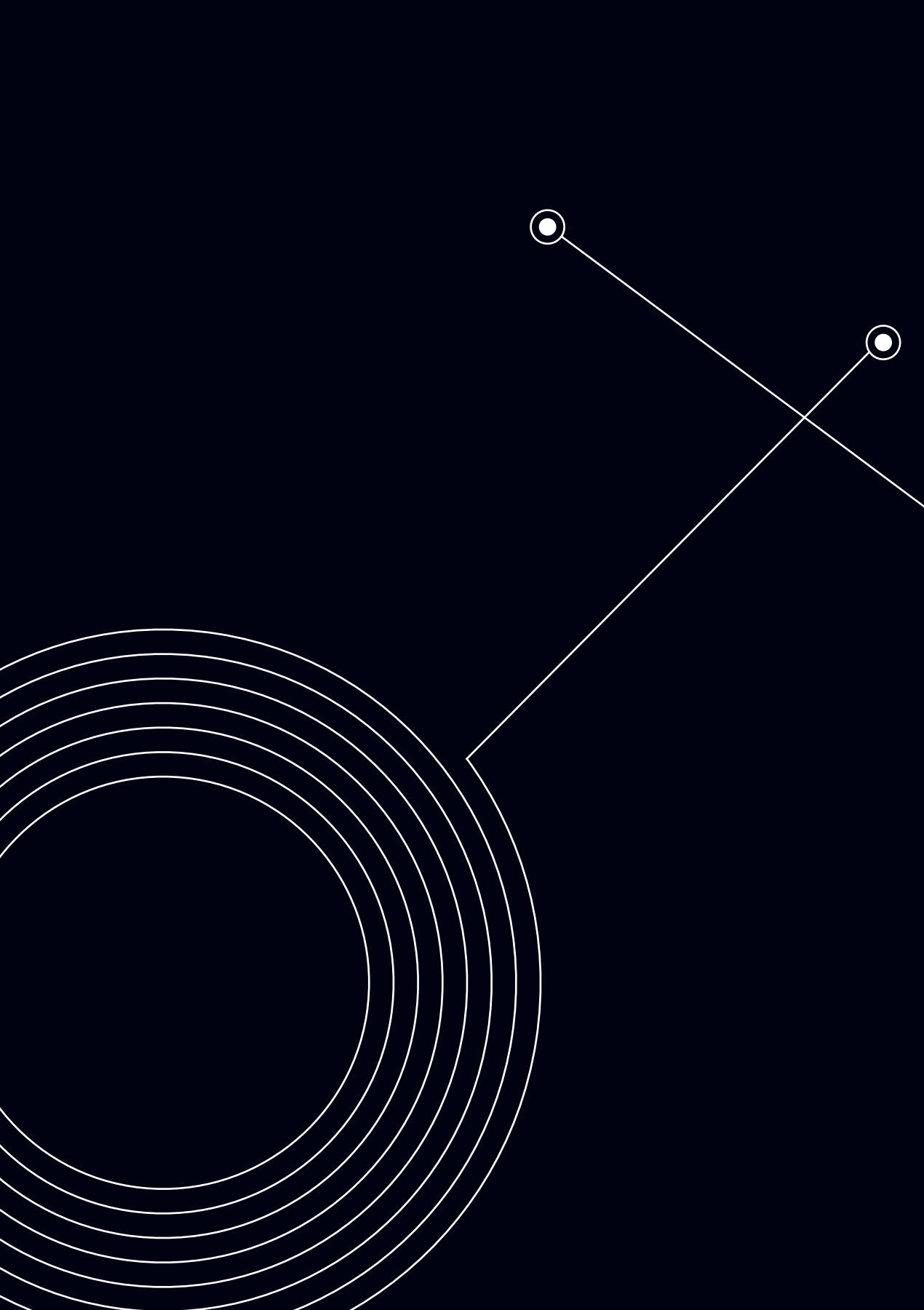
عناصر الإدارة اللازمة لمراقبة التقدم والنجاح في تنفيذ الإطار الوطني لضمان المعلومات.

تهدف الهيئة الوطنية للأمن الإلكتروني، من خلال تبني هذ الإطار، إلى ضمان توفر الحد الأدنى المطلوب من قدرات ضمان أمن المعلومات في جميع الجهات العاملة في الدولة، واستحداث منهج مشترك يتيح لها التفاعل مع بعضها بعضاً وتطبيق ضمان أمن المعلومات من منظور كل قطاع والدولة.



الفصل الثالث

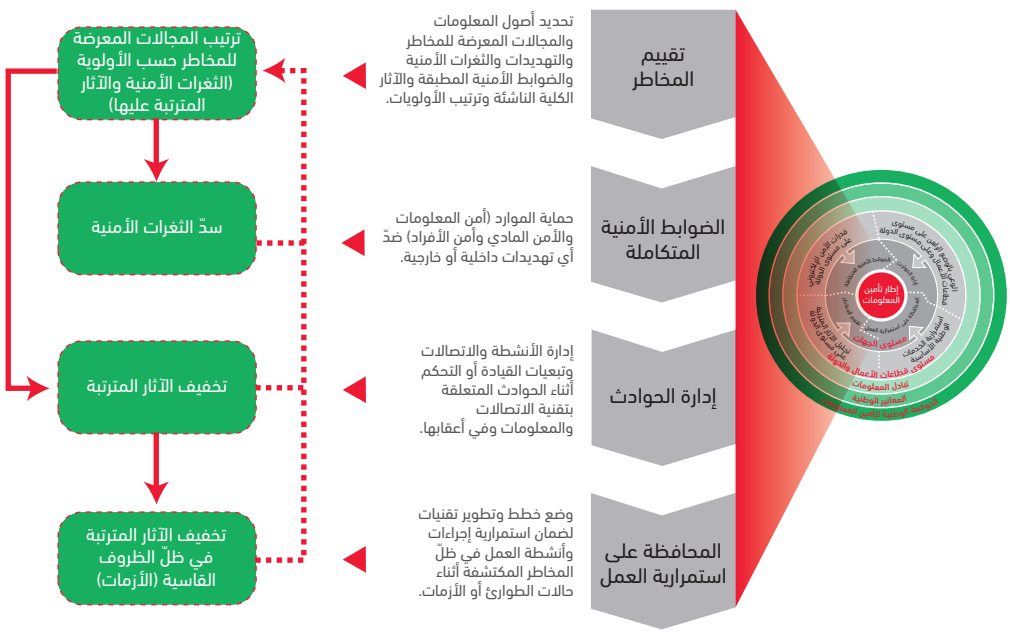
ضمان أمن المعلومات
على مستوى الجهات



٣,٠
ضمان أمن المعلومات على مستوى الجهات

يُحدد الإطار الوطني لضمان المعلومات مجموعة فرعية معينة من القدرات الأساسية اللازمة لتحقيق الحد الأدنى المطلوب من مستوى ضمان أمن المعلومات داخل كل جهة, من خلال اعتماد منهج قائم على دورة العمل. وتُحدد الهيئة الوطنية للأمن الإلكتروني بالتعاون مع الجهات المعنية الرئيسية المتطلبات التفصيلية لكل من هذه القدرات وفقاً للمعايير والمبادئ التوجيهية الوطنية المشتركة وتلك الخاصة بكل قطاع من قطاعات الأعمال المختلفة (بما فيها القطاع الحكومي أو الإدارة العامة).

الشكل التوضيحي (٣): القدرات الخاصة بالجهات في الإطار الوطني لضمان أمن المعلومات



٣,١
تقييم مخاطر أصول المعلومات

يعد تقييم المخاطر المُكون الرئيسي في المنهج الفعال لضمان المعلومات القائم على دورة العمل، حيث يساهم في تحديد المناطق الأكثر عرضة للمخاطر، ويساعد المدراء المسؤولين عن ضمان أمن المعلومات على ترتيب الموارد حسب أولويتها وتخصيصها للحد من المخاطر الشاملة بكفاءة. ويتطلب هذا الأمر اتباع منهج منظم وقابل للتكرار لتقييم حالة النظم والشبكات الإلكترونية، وإيجاد الكفاءة والتوازن بين الإنفاق على الضوابط الأمنية وبين الضرر المحتمل الناشئ عن الإخفاقات الأمنية.

وتضمن منهجية تقييم المخاطر الموضحة في هذه السياسة تطبيق منهج موحد على مستوى جميع الجهات لتحقيق نفس النتائج المنشودة، مع إتاحة المساحة التي تحتاجها كل جهة للاستفادة من إجراءاتها الحالية وتلبية احتياجات العمل الخاصة بها. ويوضح الإطار الوطني لإدارة مخاطر الأمن الإلكتروني توجيهات مفصلة أخرى للجهات الحيوية بشأن النهج والمنهجية المناسبة لإجراء تقييم المخاطر.

٣,١,١ جرد الأصول

يتعين على كل جهة أن تكون على دراية تامة بجميع أنواع أصول المعلومات (مثل الأجهزة والبرمجيات وقواعد البيانات) التي تمتلكها في وضعها الراهن وفي البنية المؤسسية في المستقبل.

٣,١,٢ تحليل الأثر المترتب على الأعمال

ينبغي على كل جهة تقييم الأثر المحتمل في حالة حدوث اختراق إلكتروني أو تعطيل عمل لأحد أصول معلوماتها، بما يتضمن فهم الأنشطة والإجراءات التي يدعمها كل أصل من أصول المعلومات.

٣,١,٣ تقييم مستوى تعرض أصول المعلومات للمخاطر

يتعين على كل جهة تقييم مستويات تعرض أصول معلوماتها المهمة للتهديدات ومدى احتمالية التعرض لاختراق أمني عبر الثغرات الأمنية.

٣,٢
الضوابط الأمنية المتكاملة

بناءً على نتائج تقييم المخاطر، تعمل الجهات على توثيق سبل التخفيف من حدة المخاطر التي يتم اكتشافها. وعلى أقل تقدير، ينبغي أن تنصّ تلك المستندات نصّاً واضحاً على مجموعة متكاملة من ضوابط أمن المعلومات والأمن المادي وأمن الأفراد التي يتم تطبيقها إضافةً إلى الأساس المنطقي لاختيار الضوابط استناداً إلى تحليل التكاليف والمزايا.

٣,٢,١ أمن النظم والشبكات

تعمل كل جهة على تحديد الضوابط الأمنية المطلوبة (مثل برمجيات الحماية والتشفير ومكافحة الفيروسات وإدارة الهوية وغيرها) لحماية أصول المعلومات التي تملكها.

٣,٢,٢ الأمن المادي

تعمل كل جهة على تحديد ضوابط الأمن المادي المطلوبة (مثل حماية الأجهزة ووضع أقفال الأبواب والأسوار المحيطة وأجهزة إنذار الحريق وغيرها) لحماية أصول المعلومات التي تملكها.

٣,٢,٣ أمن الأفراد

تعمل كل جهة على تحديد ضوابط أمن الأفراد (مثل التحري عن خلفية وسيرة الأشخاص للعمل وإعادة أصول المعلومات بعد ترك العمل وغيرها) المطلوبة لحماية أصول المعلومات التي تملكها.

٣,٣
إدارة الحوادث

من أجل تقليل أثر حوادث الأمن الإلكتروني، ينبغي أن تكون كل جهة قادرة على مراقبة أصول معلوماتها، واكتشاف وتحليل حوادث الأمن الإلكتروني لديها وتولي إدارتها، وتصعيدها إلى مستوى قطاعات الأعمال أو مستوى الدولة عند الاقتضاء مع الأخذ في الاعتبار الإطار الوطني للاستجابة لحوادث الفضاء الإلكتروني.

٣,٣,١ الوعي بالوضع الراهن

ينبغي أن تكون لدى كل جهة القدرة الذاتية على مراقبة الوضع الراهن لأصول معلوماتها، وأن تكون لديها دراية شاملة ببيئة التهديدات الإلكترونية المحيطة، ويتضمن هذا القدرة على اكتشاف حوادث الأمن الإلكتروني الداخلية، والأخذ في الحسبان أي تهديدات أو إنذارات أو معلومات بوجود حوادث ترد من مصادر خارجية.

٣,٣,٢ الاستجابة للحوادث داخل الجهات

ينبغي على كل جهة أن تقوم بتطوير القدرات الداخلية لديها للاستجابة للحوادث والسعي للتخفيف من أثر الحوادث الداخلية أو تلك الناشئة عن جهات أخرى والتي قد تؤثر فيها بشكل مباشر أو غير مباشر.

ويوضح الإطار الوطني للاستجابة لحوادث الفضاء الإلكتروني بشكل أكثر تفصيلاً المتطلبات والقدرات التي ينبغي تطبيقها من قبل الجهات الحيوية في هذا الشأن.

٣,٣,٣ تصعيد الحوادث إلى مستوى القطاع أو مستوى الدولة

تقوم كل جهة باستحداث إجراءات أو قنوات للاتصال تُصعد من خلالها الحوادث الجسيمة إلى مستوى القطاعات أو مستوى الدولة بما يتوافق مع الإطار الوطني للاستجابة للحوادث الذي تضعه الهيئة الوطنية للأمن الإلكتروني.

٣,٤
المحافظة على استمرارية العمل

بناءً على تحليل الأثر المترتب على الأعمال، ينبغي على كل جهة تحديد أصول معلوماتها التي تمثل ركيزة أساسية في سير أعمالها. وتعمل كل جهة على ضمان توفر وظائف العمل المهمة لعملائها ومورديها وغيرهم من الجهات حسب الحاجة حتى في حالة وقوع حوادث جسيمة عبر الفضاء الإلكتروني أو غيرها من أنواع الحوادث (مثل الكوارث الطبيعية) التي قد تؤثر في توفر الخدمة. ولا يقتصر تنفيذ عملية المحافظة على استمرارية العمل على وقت وقوع الكوارث فحسب، بل تتطلب تنفيذ أنشطة يومية للحفاظ على توفر الخدمة وتناسقها وإمكانية استعادتها عند الحاجة.

٣,٤,١ تخطيط المحافظة على استمرارية العمل

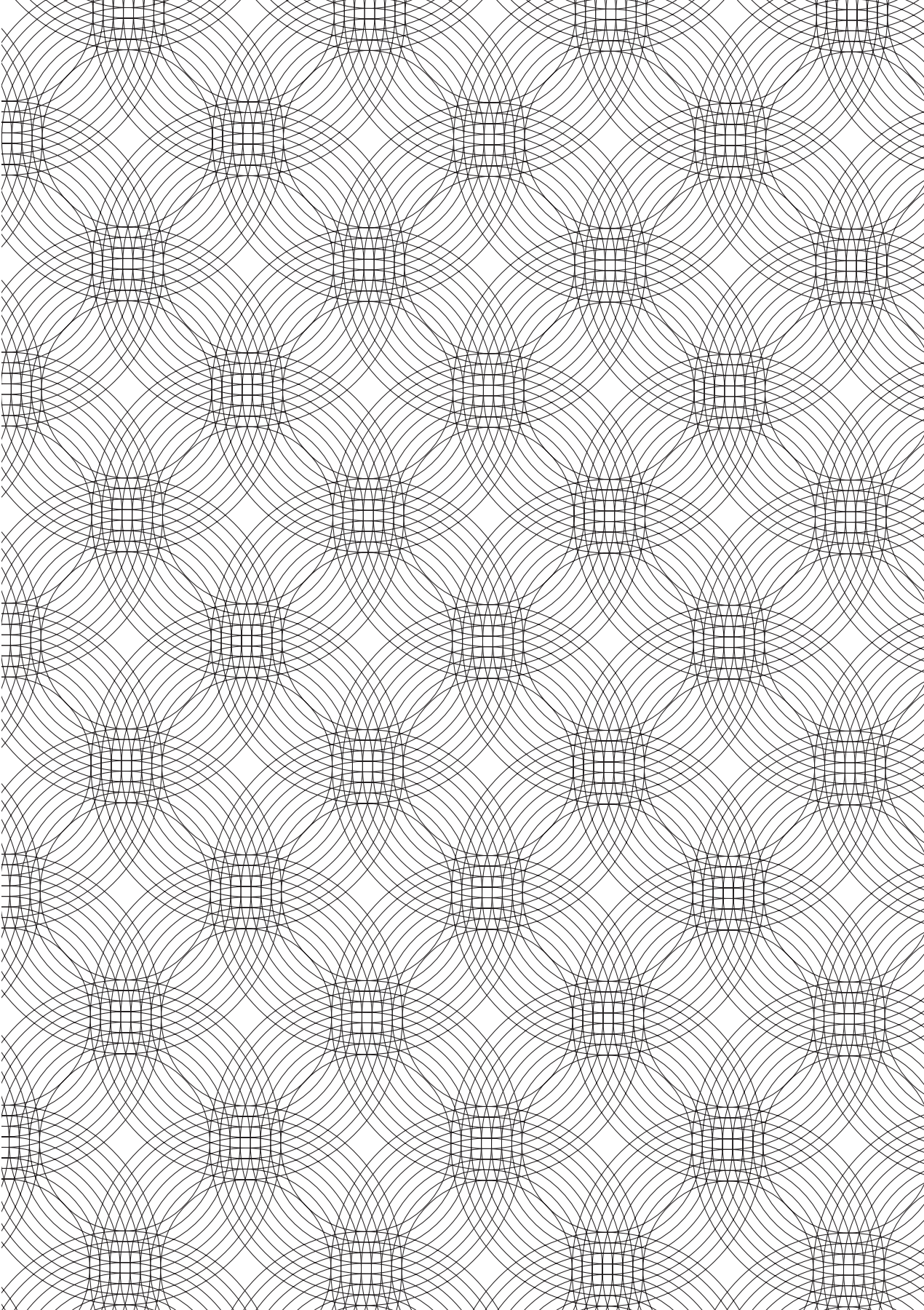
قبل وقوع أي حادث كارثي، يتعين على كل جهة وضع خطة استباقية والقيام باختبارها بانتظام لتعزيز استمرارية المعلومات ونظم المعلومات والاتصالات اللازمة للخدمات والعمليات الأساسية في ظل ظروف قاسية.

٣,٤,٢ التعافي من الكوارث

ينبغي على كل جهة أن تضع خطة داخلية للتعافي من الكوارث على أن توضح فيها عملية التعافي السريع لأصول المعلومات الحيوية عند تعرضها لتعطل بسبب حادث أو كارثة ما.

٣,٤,٣ استعادة حالة الاستقرار

ينبغي على كل جهة تحديد خطة لاستئناف الأعمال تضمن سلاسة عودة أصول المعلومات الحيوية إلى حالتها الطبيعية عقب تعطلها.



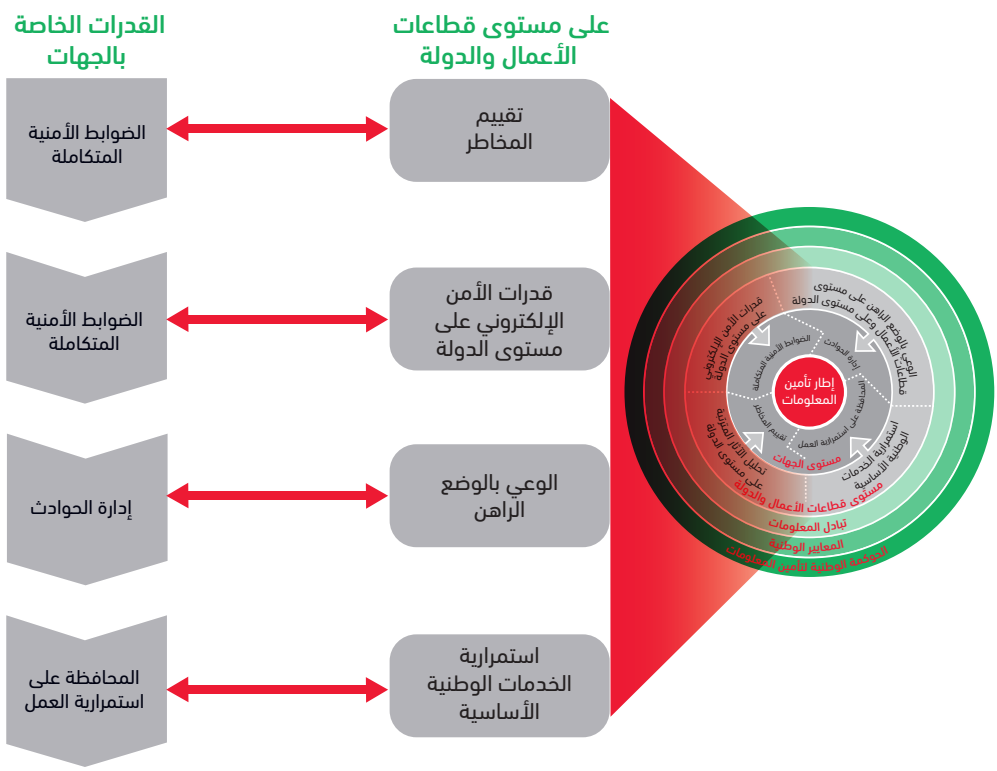
الفصل الرابع

ضمان المعلومات على مستوى القطاعات ومستوى الدولة

٤,٠
ضمان أمن المعلومات على مستوى القطاعات ومستوى الدولة

يتم دعم القدرات الخاصة بالجهات بمجموعة من مكونات القيمة المضافة التي تساعد كل جهة على تخطي محيطها الخاص والاتصال بمكونات ضمان أمن المعلومات على مستوى كل من القطاع الذي تنتمي إليه ومستوى الدولة. وتشمل هذه المكونات ما يلي:

الشكل التوضيحي(٤): مكونات سياق ضمان أمن المعلومات على مستوى كل من قطاعات الأعمال والدولة



تقييم المخاطر على مستوى كل من القطاعات والدولة

توجيه كيفية دمج مستويات المخاطر لدى الجهات لتشكيل رؤية شاملة للمخاطر على مستوى كل من قطاعات الأعمال والدولة وتحديد الأولويات المشتركة وأفضل التدابير اللازمة.

قدرات الأمن الإلكتروني على مستوى الدولة

الارتقاء بمستوى قدرات الأمن الإلكتروني لدى الجهات من خلال استفادتها من قدرات مشتركة على صعيد القطاع أو الدولة (مثل تطوير القدرات بالاعتماد على البرامج البحثية).

الوعي بالوضع الراهن على مستوى كل من قطاعات الأعمال والدولة

تبادل أنواع المعلومات المحددة مسبقاً بشكل رسمي مع الجهات المعنية على مستوى كل من القطاعات والدولة قبل وقوع الحوادث وأثنائها وفي أعقابها، والعمل سوياً للتصدي للهجمات الإلكترونية بحسب ما هو منسق مسبقاً.

استمرارية الخدمات الوطنية الحيوية

العمل مع الجهات المعنية المختلفة ومن خلال إجراءات فعالة للتقليل من وقت توقف الخدمات الوطنية الحيوية في حال وقوع الكوارث.

٤,١

تقييم المخاطر على مستوى القطاعات ومستوى الدولة

يهدف تقييم المخاطر على مستوى الدولة وكافة القطاعات إلى تزويد الجهات المعنية بفهم واضح ومشترك للمناطق الأكثر عرضة لمخاطر الأمن الإلكتروني في الدولة وترتيب تخصيص الموارد لتلك المجالات حسب الأولويات.

وتنصّ سياسة حماية البنية التحتية للمعلومات الحيوية لدولة الإمارات على منهجية عامة لتقييم المخاطر في كافة القطاعات الحيوية في الدولة. ويتم شرح هذه المنهجية وتفصيلها بشكل أدق من خلال الإطار الوطني لإدارة مخاطر الفضاء الإلكتروني الذي يضمن تطبيق منهج موحد على مستوى جميع الجهات لتحقيق نتائج مماثلة، مع إتاحة المساحة التي تحتاجها كل جهة للاستفادة من إجراءاتها الحالية وتلبية احتياجات العمل الخاصة بها، ويشمل ذلك ما يلي:

- منهجية للجهات المُشغلة لتحديد ماهية أصولها الداعمة للخدمات الوطنية الحيوية.[٢]
- إرشادات حول مستويات الثغرات الأمنية التي ينبغي وضعها في الحسبان.
- مؤشرات لأنواع أساليب التهديد المستخدمة في اختراق الثغرات الأمنية.
- إرشادات حول تحليل وتقييم المخاطر المكتشفة.
- وصف لكيفية جمع نتائج تقييم المخاطر على مستوى الجهات لتشكيل الرؤية الشاملة للمخاطر على مستوى كل القطاع والدولة.

[٢] تنصّ سياسة حماية البنية التحتية للمعلومات الحيوية على الخدمات الوطنية الحيوية.

٤,٢

قدرات الأمن الإلكتروني على مستوى الدولة

تقوم الهيئة الوطنية للأمن الإلكتروني عند الحاجة وعلى النحو الملائم بدعم الجهات المختلفة في تنفيذ منهج الأمن المتكامل من خلال مساعدتها على الوصول والاستفادة بحسب ما هو ممكن ومناسب إلى قدرات الأمن الإلكتروني على مستوى الدولة، مثل:

- القدرات التي طوّرتها جهات أخرى على مستوى الدولة.
- نماذج منتجات محددة من برامج بحثية يتم تمويلها على مستوى الدولة.
- التصاريح الأمنية الوطنية للموظفين الأساسيين ذوي العلاقة بضمان وأمن المعلومات الحيوية.
- قدرات متقدمة لمراقبة الشبكات.
- معلومات حول تطور طبيعة التهديدات.
- إمكانية الوصول إلى الجهات والقدرات الدولية.
- مواضيع محددة أخرى غير مشمولة ضمن المعايير العامة لضمان المعلومات.

واستناداً إلى نتائج تقييم المخاطر على مستوى كل من قطاعات الأعمال والدولة، تقوم الهيئة الوطنية للأمن الإلكتروني بتحديد المجالات ذات الأولوية التي تحتاج إلى توفير قدرات محددة للأمن الإلكتروني الوطني.

٤,٣

الوعي بالوضع الراهن على مستوى القطاعات والدولة

في ظل إدارة الجهات المختلفة لحوادثها الداخلية، يتعين عليها أيضاً إدراك الأنشطة المنفذة في البيئة المحيطة بها وتبادل المعلومات مع الجهات المعنية الأخرى قبل وقوع الحوادث الجسيمة وأثنائها وفي أعقابها.

تعمل الهيئة الوطنية للأمن الإلكتروني على تعزيز الوعي على مستوى كل من قطاعات الأعمال المختلفة (بما في ذلك القطاع الحكومي والإدارة العامة) والدولة من خلال توفير إمكانية تبادل معلومات موثوقة تتيح للجهات المختلفة إمكانية تبادل المعلومات على مستوى كل قطاع، وتُتيح بالمثل لجميع القطاعات إمكانية تبادل المعلومات على مستوى الدولة، وتفصل السياسة الوطنية لتبادل المعلومات الإجراءات والقدرات الخاصة.

سيوفر الإطار الوطني للاستجابة لحوادث الفضاء الإلكتروني التوجيه اللازم للجهات المختلفة بشأن كيفية تقييم الأثر المترتب على خرق سرية المعلومات أو سلامتها أو توفرها، وكيفية تصعيد هذه الحوادث إلى مستوى القطاعات والدولة.

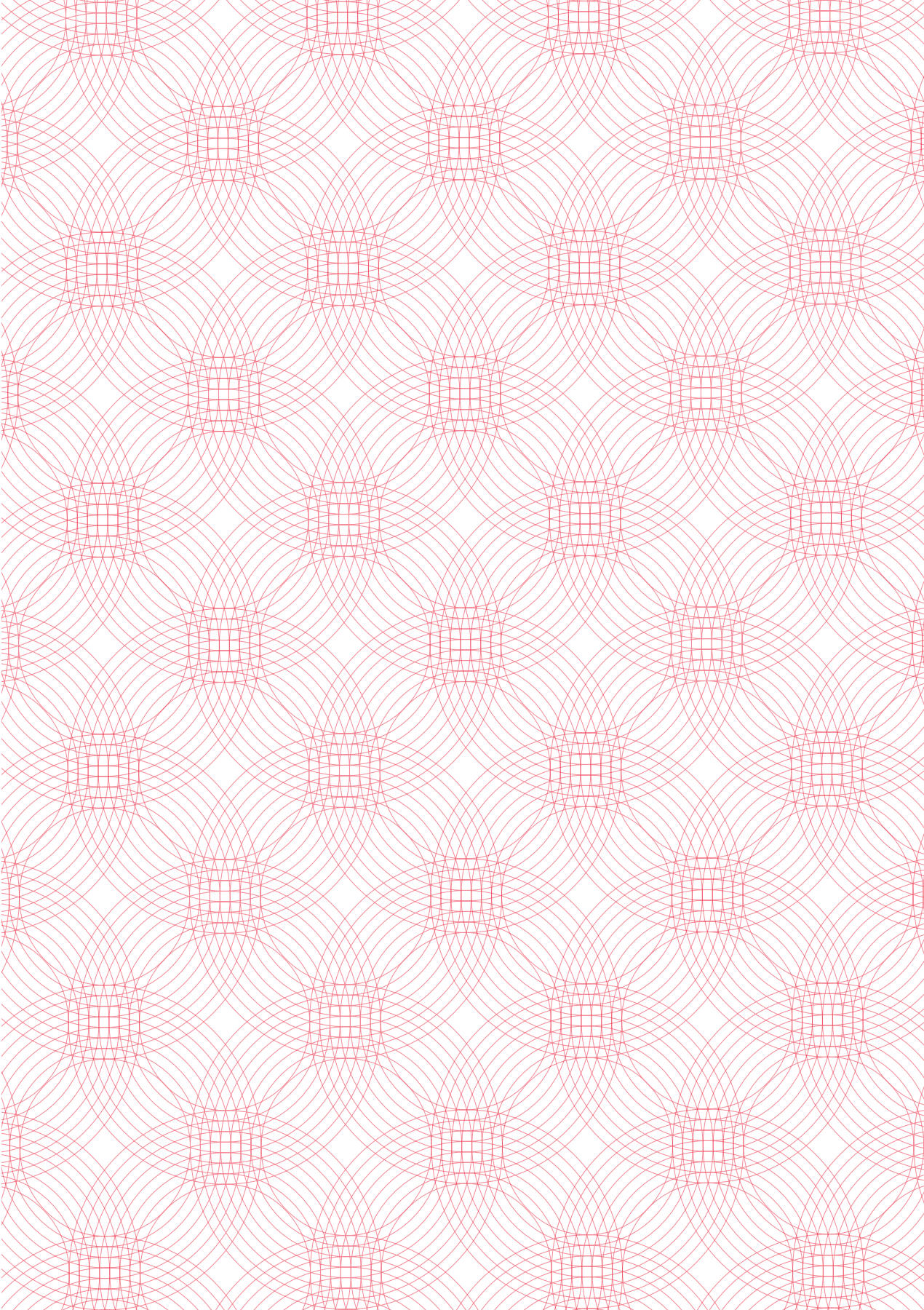
٤,٤

استمرارية الخدمات الوطنية الأساسية

تتولى كل جهة، إضافةً إلى ضمان استمرارية خدماتها وعملياتها الأساسية الخاصة بها، مسؤولية ضمان استمرارية عمل البنية التحتية للمعلومات الحيوية التي تديرها أو تشغلها هذه الجهة والتي ترتكز عليها خدمات وطنية حيوية . لذا، تنبغي مراعاة المتطلبات الوطنية في إطار عملية التخطيط للمحافظة على استمرارية العمل داخل كل جهة من الجهات، عند وضع المعايير المستخدمة في تحديد قدرات النَسخ الاحتياطي والتعافي من الحوادث والكوارث على المدى القريب والبعيد واستئناف الأعمال.

ستوفر الهيئة الوطنية للأمن الإلكتروني بالتعاون مع الهيئات التنظيمية للقطاع والجهات المعنية الرئيسية ذات الصلة، الإرشادات اللازمة بشأن استمرارية الخدمات الوطنية الحيوية بما في ذلك:

- معلومات حول حساب النقطة المستهدفة لاستعادة القدرة على العمل، والوقت المستهدف لاستعادة القدرة على العمل للخدمات الوطنية الحيوية.
- متطلبات التعافي من الكوارث للنظم الداعمة للخدمات الوطنية الحيوية.
- متطلبات الإبلاغ عن استعادة الحالة المستقرة للخدمات الوطنية الأساسية.
- أي توجيهات داعمة أخرى ذات صلة.



الفصل الخامس

تبادل المعلومات

٥,٠
تبادل المعلومات

يشير تبادل المعلومات إلى تداولها فيما بين مجموعات الجهات المعنية، ويُعد عنصراً محورياً وممكناً مهماً فيما يتعلق بكفاءة قدرات إدارة الأمن الإلكتروني على مستوى الدولة، حيث يعتبر حلقة الوصل التي تربط جميع الجهات الفاعلة في كل قطاع وعلى مستوى الدولة ككل؛ فهو إحدى الركائز الرئيسية التي تُميز الإطار الوطني لضمان المعلومات عن غيره من الأطر القائمة بذاتها في هذا السياق. ويهدف مُكون تبادل المعلومات الخاص بالإطار الوطني لضمان المعلومات إلى نشر معلومات حول التهديدات الإلكترونية وأفضل الممارسات المتبعة في ضمان أمن المعلومات وذلك فيما بين الجهات المعنية المشاركة سعياً لتعزيز قدرتها على حماية أصول المعلومات على النحو الأمثل.

وتصف السياسة الوطنية لتبادل المعلومات البيئة والنموذج الوطني لتبادل المعلومات الخاصة بالأمن الإلكتروني لدولة الإمارات، كما توضح تفاصيل متطلبات بيئة ومنصة تبادل المعلومات على مستوى الدولة، بما يتضمن ما يلي:

الجهات المشاركة

على ثلاثة مستويات من التفاعل؛ الجهة والقطاع والدولة. ويوفر هذا النموذج صاحب المستويات بنية لتبادل المعلومات يمكن إدارتها والتي تسهل عملية تبادل المعلومات حول موضوعات الأمن الإلكتروني عبر الجهات وعبر قطاعات الأعمال المختلفة (بما في ذلك القطاع الحكومي والإدارة العامة).

الخدمات المقدمة

تشمل العديد من خدمات تبادل المعلومات، بما في ذلك تصفية الرسائل التحذيرية والوساطة الاستشارية والإبلاغ عن الحوادث.

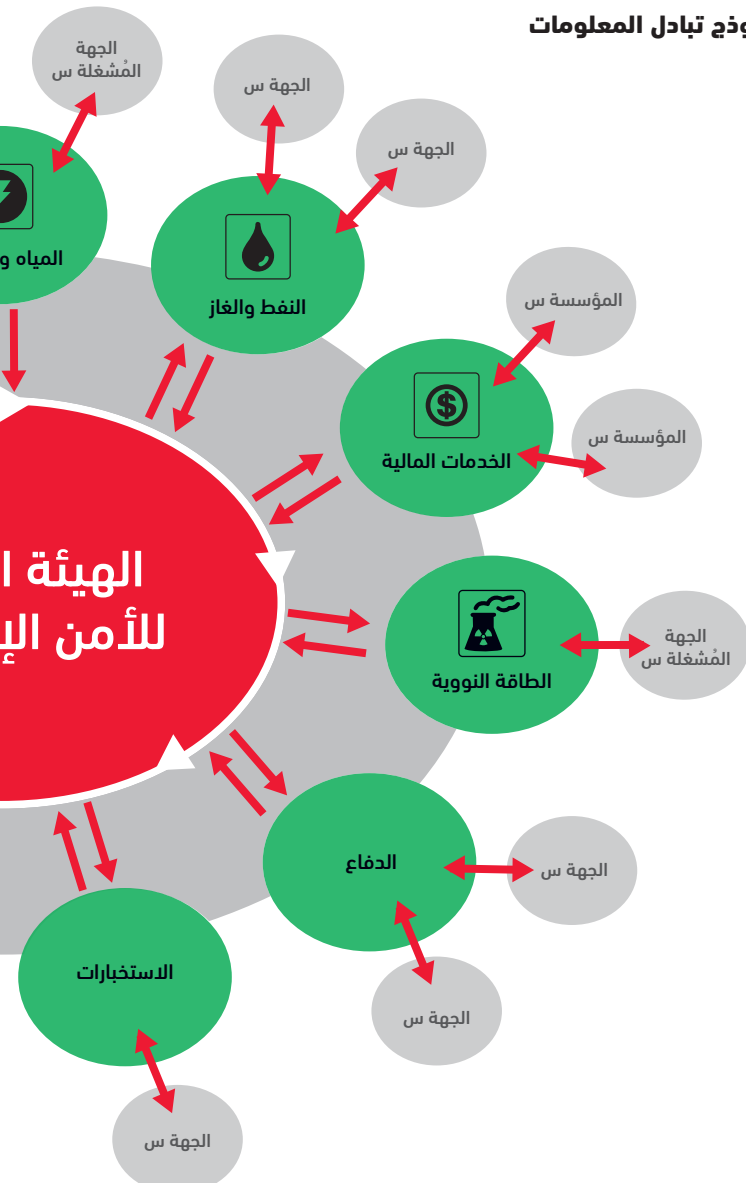
السمات الرئيسية

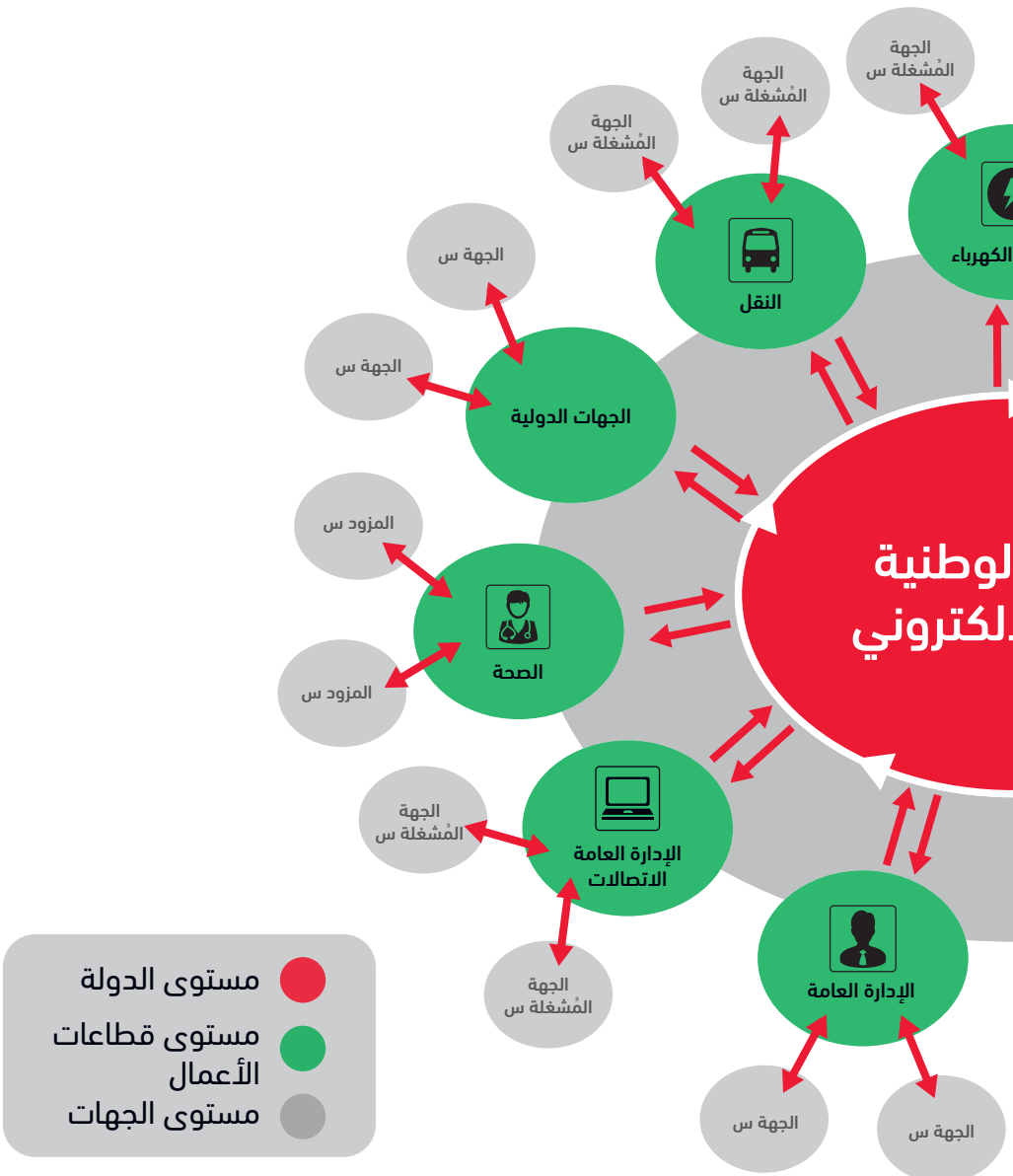
ضرورية لنجاح تطبيق نموذج تبادل المعلومات مثل المنصة الآمنة وإخفاء الهوية وتحكم مالك (الجهة صاحبة المعلومات) في حقوق المعلومات.

نموذج التشغيل

يشير إلى أهم متطلبات الأعمال والمتطلبات الوظيفية.

الشكل التوضيحي (٥) : مفاهيم نموذج تبادل المعلومات




الوطنية
لكتروني
الكهرباء
النقل
الجهات الدولية
الصحة
الإدارة العامة الاتصالات
الإدارة العامة
الجهة المُشغلة س
الجهة س
المزود س
مستوى الدولة
مستوى قطاعات الأعمال
مستوى الجهات

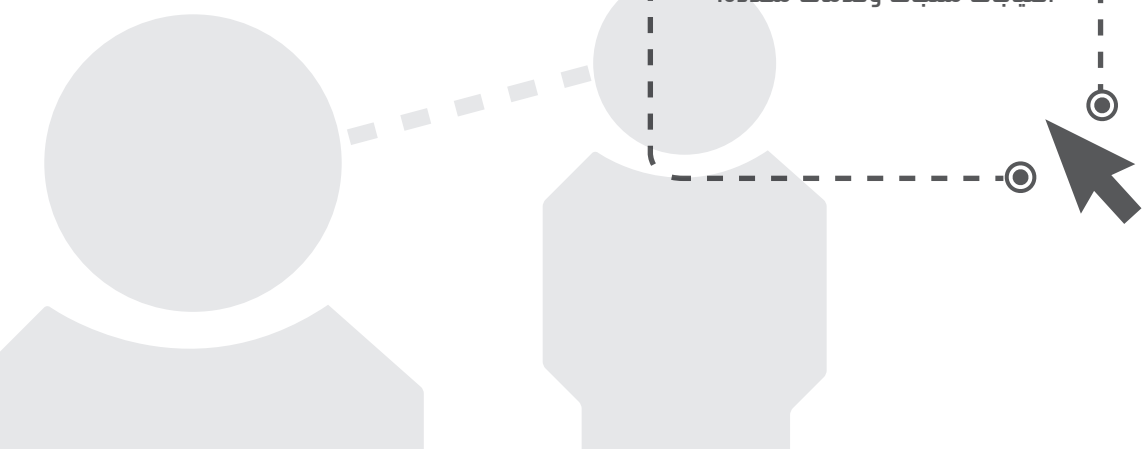
الفصل السادس

المعايير الوطنية لضمان أمن المعلومات

٦,٠
المعايير الوطنية لضمان أمن المعلومات

تُضاف المعايير الوطنية إلى المعايير المطبقة من قبل الجهات بغية الارتقاء بمستوى ضوابط وقدرات ضمان أمن المعلومات داخل جميع الجهات إلى الحد العام المطلوب، وتعمل المعايير على إيجاد الممكنات والعناصر المطلوبة لربط تلك الجهات الفاعلة بعضها ببعض داخل القطاع الواحد وعلى مستوى الدولة.
ونستعرض فيما يلي المستويات الثلاثة للمعايير الوطنية لدولة الإمارات:

- المعايير العامة: هي تلك المعايير التي تسري على جميع الجهات وفي القطاعات المختلفة.
- المعايير الخاصة بقطاع محدد: هي معايير ضمان أمن المعلومات التي تغطي النواحي والخصائص والمتطلبات المميزة لكل قطاع على حدة.
- المعايير الخاصة بالخدمات والمنتجات: هي المعايير المُصممة خصيصاً لتلبية احتياجات منتجات وخدمات محددة.



وستقوم الهيئة الوطنية للأمن الإلكتروني بمراجعة هذه المعايير بهدف التحقق من فعاليتها وملاءمتها بشكل دوري أو كلما تطلبت الحاجة.

٦,١
المعايير العامة

تُحدد المعايير العامة الحد الأدنى المطلوب من قدرات ضمان أمن المعلومات وضوابط الأمن الإلكتروني التي ينبغي على كل جهة عاملة في الدولة أن تسعى إلى تحقيقها، وبالنسبة للجهات الحيوية، يكون الامتثال لتلك المعايير أمراً إلزامياً. حيث تُحدد هذه المعايير المتطلبات الإدارية والتقنية (والتشغيلية) العامة التي ينبغي على كل جهة أن تطبقها، بغض النظر عن القطاع الذي تعمل فيه الجهة أو النشاط الذي تمارسه.

ويتعين على جميع الجهات الحكومية وغيرها من الجهات التي تصنفها الهيئة الوطنية للأمن الإلكتروني على أنها جهة "حيوية" في القطاعات الحيوية المختلفة الامتثال الى جميع المعايير العامة.

٦,٢
المعايير الخاصة بقطاع محدد

يتمتع كل قطاع بخصائص فريدة وتعقيدات تشغيلية قد تختلف عن غيره من القطاعات. وبناءً على هذا، قد يكون التباين كبيراً بين القطاعات في أنواع تهديدات وثغرات الأمن الإلكتروني التي ينبغي على الجهات المختلفة التصدي لها وإدارة مخاطرها. فعلى سبيل المثال، تمثل نظم التحكم الصناعية المستخدمة في قطاع الكهرباء تحديات للأمن الإلكتروني لا يواجهها القطاع المالي.

وللتغلب على التحديات الخاصة التي تواجه كل قطاع، تقوم الهيئة الوطنية للأمن الإلكتروني بوضع معايير خاصة بكل قطاع حسب الحاجة وبالتشاور مع الجهات المنظمة والقيادية بالإضافة إلى الجهات العاملة في القطاع والمشغلين. وفي بعض الحالات الخاصة، قد تُقرر الجهات المُنظمة إصدار إرشادات تقنية إضافية لمساعدة الجهات على تنفيذ معايير القطاع الخاصة بها.

تحديد آلية تعاون هيئة الأمن الإلكتروني والجهات المُنظمة المعنية والجهات العاملة في القطاعات لتطوير وتنفيذ تلك المعايير.

[٣] تنصّ سياسة حماية البنية التحتية للمعلومات الحيوية لدولة الإمارات الصادرة عن الهيئة الوطنية للأمن الإلكتروني على الجهات التي تُصنف على أنها "جهة حيوية".

٦,٣

المعايير الخاصة بالخدمات والمنتجات

تقوم الهيئة الوطنية للأمن الإلكتروني، عند الحاجة، بوضع معايير مُخصصة للخدمات والمنتجات. وبناءً على التنسيق مع الجهات المعنية، تقوم الهيئة بتحديد الحاجة إلى تطبيق تلك المعايير ونوعية ومستوى الضوابط الأمنية المطلوبة. ونظراً للطبيعة المؤقتة لتلك المعايير، يُحدد كل معيار نطاق تطبيقه.

٦,٤

التحقق من الامتثال وإصدار الشهادات

تقوم الهيئة الوطنية للأمن الإلكتروني بالتحقق من الامتثال للمعايير الوطنية من قبل الجهات الحيوية ومن ثم قد تصدر شهادات خاصة بذلك. وتنصّ السياسة الوطنية الخاصة بالامتثال للمعايير وإصدار الشهادات على كيفية قيام الهيئة بالتحقق من مستويات الامتثال وتصنيفها وفقاً لمتطلبات التنفيذ أو الجودة أو كليهما على النحو الوارد في المعايير الوطنية. ويغطي برنامج التحقق من الامتثال وإصدار الشهادات المعايير الوطنية المطبقة على الأفراد والمنظمات والنظم والخدمات والمنتجات.

تتألف عملية التحقق من الامتثال وإصدار الشهادات من ثلاث خطوات رئيسية:

الشكل التوضيحي (٦): عملية التحقق من الامتثال

الخطوة	الأنشطة الرئيسية
المبادرة	**الأمن المعلوماتي المخصص حسب** • المؤسسات • الأشخاص • الأنظمة • المنتجات / الخدمات
التقييم	**التقييم** • تصميم وتنفيذ الخطط الأمنية المتعلقة بالمنتجات، الأسس والخدمات من خلال إجراء الاختبارات، تقييم المخاطر وغير ذلك • المعرفة والمهارات الخاصة بالمؤسسات والأشخاص
الترخيص والتأكيد	**اتخاذ القرار بشأن الموافقة على التأهيل أو الرفض** • تقديم الشهادات لإدارة المنتجات، الخدمات أو البنى التحتية • تقديم شهادات الجودة للأشخاص أو المؤسسات

تنصّ السياسة الوطنية للتحقق من الامتثال للمعايير على الأنشطة التفصيلية المنفذة في كل خطوة من عملية التحقق من الامتثال وإصدار الشهادات في هذا الشأن.

٦,٠
المنتديات التقنية لضمان المعلومات

توفر المنتديات التقنية لضمان المعلومات التي تقودها وتنظمها الهيئة الوطنية للأمن الإلكتروني منصة للجهات لتبادل الخبرات في تطبيق المعايير الوطنية لضمان المعلومات والدروس المستفادة. بالإضافة إلى التعبير عن التحديات التي قد تواجههم وطلب التوضيحات فيما يتعلق بضمان المعلومات وتطبيق المعايير. ويشارك في المنتديات التقنية لضمان المعلومات الشركاء الأساسيون في مجال ضمان أمن المعلومات كالجهات القيادية والمنظمة والجهات العاملة والمشغلين الرئيسيين في كل قطاع، ويدعى كذلك الى المشاركة في المنتدى المعنيون من الأوساط الأكاديمية والشركات الخاصة (كالبائعة والاستشارية) والخبراء التقنيون, للمناقشة والمراجعة العامة لسياسات ومعايير ضمان أمن المعلومات وتعزيز تطبيقها على مختلف المستويات. وستساهم المنتديات كذلك في زيادة مستوى الوعي والمعرفة بالأمن الإلكتروني من خلال استعراض أحدث التطورات وتقنيات الجيل القادم في مجال ضمان أمن المعلومات وكيفية استفادة القطاعين العام والخاص منها.

الفصل السابع

حوكمة ضمان أمن المعلومات على مستوى الدولة

٧,٠
حوكمة ضمان أمن المعلومات على مستوى الدولة

يوضح نموذج حوكمة الإطار الوطني لضمان أمن المعلومات آلية تفاعل الهيئة الوطنية للأمن الإلكتروني مع الجهات المعنية ومراقبة الامتثال لمتطلبات الإطار الوطني، ويتضمن ذلك ما يلي:

- الأسلوب الذي ستستخدمه الهيئة في التواصل والتفاعل مع الجهات المعنية بشأن تنفيذ الإطار الوطني.
- الأثر الذي قد يترتب على مؤسسات الجهات المعنية حتى تتمكن من الإيفاء بمتطلبات الإطار الوطني (على سبيل المثال ضرورة توفر نقطة اتصال في مؤسسات الجهات المعنية).
- التوقعات بشأن متطلبات الجهات المعنية التي ترفع تقاريرها إلى الهيئة.
- الأدوات التي تستخدمها الهيئة لتعزيز مستوى الامتثال وضمانه.

٧,١

تفاعل الجهات المعنية مع الهيئة الوطنية للأمن الإلكتروني

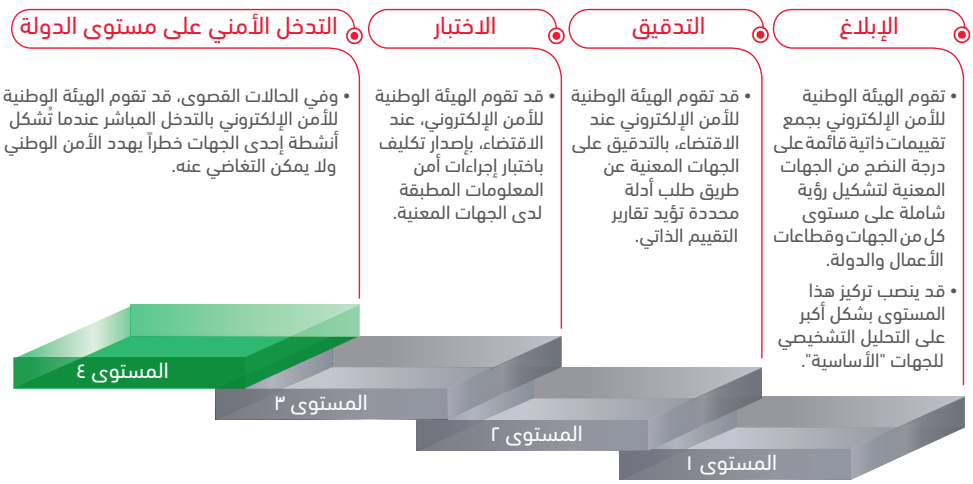
بهدف إدارة تنفيذ الإطار الوطني لضمان المعلومات بكفاءة، يتعين على الهيئة الوطنية للأمن الإلكتروني التواصل والتنسيق مع مجموعة كبيرة من جهات أساسية ذات صلة. ولتيسير هذا الأمر، ينبغي على كل جهة تعيين شخص واحد على الأقل بصفته ضابط ارتباط (منسق مركزي) مسؤول على التنسيق مع الهيئة الوطنية للأمن الإلكتروني وغيرها من الجهات الحكومية. وتقوم الجهات المعنية بإخطار الهيئة باسم ضابط الارتباط وبيانات اتصاله.

ويوضح نموذج حوكمة الإطار الوطني لضمان المعلومات على شروط اختيار ضابط الارتباط في كل جهة.

٧,٢
مراقبة الامتثال

يوضح نموذج حوكمة الإطار الوطني لضمان المعلومات تفاصيل كل مستوى من المستويات الأربعة لمراقبة الامتثال التي ستستخدمها الهيئة لإدارة امتثال الجهات المعنية على نطاق جميع جوانب الإطار الوطني، كما هو مبين في الشكل التوضيحي أدناه.

الشكل التوضيحي (٦): تصعيد مخططات مراقبة الامتثال



ويوضح نموذج حوكمة الإطار الوطني لضمان المعلومات الشروط التي ستحدد الهيئة بمقتضاها معايير تصعيد مستوى مراقبة الامتثال في جهة أو قطاع بعينه.

الملاحق

الملحق ا

الآليات الداعمة للإطار الوطني لضمان أمن المعلومات

مكونات الإطار الوطني لضمان المعلومات	الآليات الداعمة
ضمان أمن المعلومات على مستوى الجهات	• تُحدد لاحقاً
ضمان المعلومات على مستوى قطاعات الأعمال والدولة	• المبادئ التوجيهية الوطنية لإدارة المخاطر لدولة الإمارات • الإطار الوطني للاستجابة لحوادث الفضاء الإلكتروني • سياسة دولة الإمارات لحماية البنية التحتية للمعلومات الحيوية
تبادل المعلومات	• السياسة الوطنية لتبادل معلومات الأمن الإلكتروني
المعايير الوطنية	• الإطار الوطني للتحقق من الامتثال للمعايير الوطنية وإصدار الشهادات والاعتمادات
حوكمة ضمان أمن المعلومات على مستوى الدولة	• نموذج حوكمة الإطار الوطني لضمان المعلومات لدولة الإمارات

الملحق ٢
التعريفات الرئيسية

المصطلح	التعريف
خدمة حيوية [٤]	خدمة مهمة قد يكون لتعطيلها أو تدميرها أثر بالغ من الناحية الأمنية أو الاقتصادية أو الاجتماعية أو مزيج منها على دولة الإمارات.
الأمن الإلكتروني	مجموعة من القدرات (بما في ذلك النهج والممارسات والتكنولوجيات) التي صممت بهدف حماية الأصول الإلكترونية (بما في ذلك المعلومات) من النفاذ غير المشروع أو الاختراق أو التعطيل. سياق الجهة: يشير إلى مجموعة من أصول المعلومات للجهة والممارسات والمعايير التي تميز القدرات الأساسية للأمن الإلكتروني لإقامة حد أدنى لأمن المعلومات داخل جهة من الجهات.
الفضاء الإلكتروني	مجال ضمن بيئة المعلومات يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات والاتصالات بما في ذلك الإنترنت وشبكات الاتصالات السلكية واللاسلكية وأنظمة الكمبيوتر وأجهزة المعالجة والتحكم [٥].
الاستراتيجية الوطنية للأمن الإلكتروني	برنامج دولة الإمارات العربية المتحدة لحماية الفضاء الإلكتروني الوطني والحفاظ على أمنه.
أصول المعلومات	أصول مادية أو افتراضية لنظم تكنولوجيا المعلومات والاتصالات مثل البيانات والنظم والمنشآت والشبكات وأجهزة الحواسب الآلية.

ضمان أمن المعلومات	ممارسة حماية المعلومات وإدارة المخاطر واستمرارية الأعمال المتعلقة باستخدام ومعالجة وتخزين ونقل المعلومات أو البيانات والنظم والعمليات المستخدمة لهذه الأغراض. ويعتبر أمن المعلومات جزءاً من مفهوم ضمان أمن المعلومات الذي يشمل نطاقاً أعرض من مفاهيم حماية وإدارة المعلومات مثل إدارة استمرارية المعلومات، والتعافي من الكوارث، ومراقبة الامتثال، وإصدار الشهادات والاعتمادات وغيرها.
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.
الإطار الوطني لإدارة الحوادث (الإلكترونية)	برنامج وطني (يشمل السياسات والآليات والخطط والنظم) مُصمم خصيصاً لتعزيز الوعي بالوضع الراهن، وسرعة اكتشاف وتحليل الحوادث وتنسيق الاستجابة مع الجهات الوطنية المعنية بالأمن الإلكتروني.
المشغل	جهة تنشط في قطاع أعمال معين (أو سوق).
المنظم	هيئة حكومية تضع اللوائح وتراقب امتثال وسلوك الجهات الخاضعة للتنظيم في قطاع أعمال معين (أو سوق).

[٤] سيتم تبيان المعايير المفصلة المستخدمة لتحديد الخدمة الحيوية في المرحلة الأولى من عملية سياسة حماية البنية التحتية الحيوية للمعلومات لدولة الإمارات

[٥] تعريف قريب جداً من تعريف وزارة الدفاع الأمريكية