الإستراتيجية الوطنية للأمن السيبراني للطيران المدني

الفهرس

1. الإستراتيجية الوطنية للأمن السيبراني للطيران المدني 1
رسالة رئيس مجلس إدارة الهيئة العامة للطيران المدني 3
رسالة المدير العام للهيئة العامة للطيران المدني 4
1. مقدمة 5
2. الغرض من استراتيجية الأمن السيبراني الوطنية في دولة الإمارات العربية المتحدة 5
3. إدارة مخاطر الأمن السيبراني للطيران 6
4. مجلس الأمن السيبراني لحكومة دولة الامارات: 6
5. الاستراتيجية الوطنية للأمن السيبراني لدولة الإمارات العربية المتحدة: 7
1. قوانين ولوائح الأمن السيبراني: 7
2. نظام بيئي نشط للأمن السيبراني: 7
3. خطة وطنية للاستجابة للحوادث: 7
4. برنامج حماية معلومات البنية التحتية الحيوية: 7
5. شراكات: 7
6. استراتيجية الأمن الالكتروني في مجال الطيران لمنظمة الطيران المدني الدولي: 8
7. رؤية الهيئة العامة للطيران المدني الوطنية للأمن السيبراني للطيران: 8
8. الاستراتيجية العامة للهيئة العامة للطيران المدني: 8
9. فريق عمل الهيئة العامة للطيران المدني للأمن السيبراني لقطاع الطيران المدني: 9
1.9 *أهداف استراتيجية الأمن السيبراني الوطني للطيران المدني للهيئة العامة للطيران المدني:* 9
10. ركائز استراتيجية الأمن السيبراني الوطني للطيران المدني للهيئة العامة للطيران المدني: 9
1. التعاون الدولي والشراكة 10
2. الحوكمة 10
3. التشريعات واللوائح الفعالة 10
4. سياسة الأمن السيبراني 11
5. تبادل المعلومات 11
6. إدارة الوقائع والتخطيط للطوارئ 11
7. بناء القدرات والتدريب وترسيخ ثقافة الأمن السيبراني 11

الإستراتيجية الوطنية للأمن السيبراني للطيران المدني

رسالة رئيس مجلس إدارة الهيئة العامة للطيران المدني

الهدف من الاستراتيجية الوطنية للأمن السيبراني لدولة الإمارات العربية المتحدة هو إنشاء بنية تحتية إلكترونية آمنة وقوية في دولة الإمارات العربية المتحدة تمكن مواطنيها والمقيمين وأصحاب المصلحة من تحقيق تطلعاتهم وتمكين الشركاء من الازدهار في بيئة آمنة ومأمونة، ويتولى مجلس الأمن السيبراني لحكومة دولة الإمارات العربية المتحدة مسؤولية تطوير والإشراف على استراتيجية الأمن السيبراني التي تعزز بنية تحتية سيبرانية آمنة ومرنة في الدولة وتطوير استراتيجية شاملة للأمن السيبراني وإنشاء بنية تحتية سيبرانية آمنة وقوية في دولة الإمارات العربية المتحدة. ترتكز الاستراتيجية على 5 محاور وعدد من المبادرات التي تهدف إلى تفعيل منظومة الأمن السيبراني بالكامل في دولة الإمارات العربية المتحدة.

تماشياً مع الاستراتيجية الوطنية للأمن السيبراني لدولة الإمارات العربية المتحدة، قامت الهيئة العامة للطيران المدني بتطوير استراتيجية الطيران المدني الخاصة بها لمكافحة التهديدات التي يشكلها الأمن السيبراني على عمليات الطيران المدني في دولة الإمارات العربية المتحدة، وتُعرف باسم " الاستراتيجية الوطنية للأمن السيبراني للطيران المدني ".

إن استراتيجية الأمن السيبراني الجديدة هي خطتنا لضمان بقاء دولة الإمارات العربية المتحدة واثقة وقادرة ومرنة قبل كل شيء في هذا العالم الرقمي سريع الحركة، ونحن نواصل التكيف والابتكار والاستثمار من أجل حماية وتعزيز مصالح الطيران المدني لدولة الإمارات العربية المتحدة في الفضاء الإلكتروني.

معالي عبد الله بن طوق المري
وزير الاقتصاد
رئيس مجلس إدارة الهيئة العامة للطيران المدني

رسالة المدير العام للهيئة العامة للطيران المدني

أنا فخور بتقديم الإستراتيجية الوطنية للأمن السيبراني للهيئة العامة للطيران المدني، ستوجه هذه الوثيقة جهودنا الجماعية لتحديد أولويات تدابير الأمن السيبراني في مجال الطيران المدني على مدى السنوات المقبلة.

تتوافق الإستراتيجية الوطنية للأمن السيبراني للهيئة العامة للطيران المدني مع الإستراتيجية الوطنية للأمن السيبراني لدولة الإمارات العربية المتحدة وتدعمها، وتحدد مسارات واضحة لتطوير وتحسين وضع الأمن السيبراني للهيئة العامة للطيران المدني، وحماية أنظمة الطيران المدني، وبناء قدرتنا على مواجهة بيئة الأمن السيبراني المتغيرة باستمرار من خلال الشراكات التعاونية.

مع مرور كل عام، يتزايد حجم التهديد السيبراني بصورة مستمرة ويمكن أن تكون الهجمات السيبرانية مأثرة ومكلفة للغاية بالنسبة لعمليات الطيران المدني. بالإضافة إلى الأضرار المالية التي تتكبدها الكيانات، يمكن أن يؤدي ذلك أيضًا إلى إلحاق ضرر لا يحصى بسمعة أي منظمة. أصبحت الهجمات السيبرانية هذه الأيام مدمرة بشكل تدريجي ويستخدم مجرمو الإنترنت طرقًا أكثر تطوراً لشن هذه الهجمات.

تتمثل رؤية الأمن السيبراني للطيران الوطني للهيئة العامة للطيران المدني ضمان بقاء قطاع الطيران المدني في دولة الإمارات العربية المتحدة آمنًا وموثوقًا ومستدامًا ومقاومًا للهجمات السيبرانية. ويتم تحقيق ذلك من خلال الاعتراف بالالتزامات المنصوص عليها في اتفاقية الطيران المدني الدولي (اتفاقية شيكاغو) لضمان سلامة وأمن واستمرارية الطيران المدني، مع مراعاة الأمن السيبراني.

الهدف من استراتيجية الأمن السيبراني للهيئة العامة للطيران المدني هو أن يكون لدى صناعة الطيران المدني تدابير تخفيفية قوية ومرنة وديناميكية للحد من المخاطر السيبرانية المحتملة، مدعومة بخطة رقابة تنظيمية متناسبة متفق عليها. وهذا سيمكن أصحاب المصلحة في صناعة الطيران المدني من استغلال فوائد الفضاء الإلكتروني دون المساس بسلامة الطيران وأمنه والملاحة الجوية واستمرارية الخدمات.

سعادة سيف محمد السويدي
مدير عام الهيئة العامة للطيران المدني

1. مقدمة

يعتمد قطاع الطيران المدني في دولة الامارات العربية المتحدة بشكل متزايد على توافر نظم تكنولوجيا المعلومات والاتصالات وكذلك على سلامة وسرية البيانات، أما التهديدات التي تشكلها الوقائع الإلكترونية المحتملة ضد قطاع الطيران المدني فتتطور بشكل مستمر حيث أن الجهات الفاعلة التي تقف وراء التهديدات تركز على تنفيذ النوايا الخبيثة وتعطيل استمرارية العمليات وسرقة المعلومات بدوافع سياسية أو مالية أو غيرها، ومع الأخذ في الاعتبار أن التهديدات التي يتعرض لها الطيران المدني تتطور بسرعة وبشكل مستمر، يظل الطيران هدفاً لمرتكبي الجرائم في المجال السيبراني و المجال المادي، وأن التهديد السيبراني يمكن أن يتطور ليؤثر على أنظمة الطيران المدني الحيوية في جميع أنحاء العالم. ويغطي الأمن السيبراني للطيران مجموعة واسعة من مجالات الطيران المدني الدولي مثل سلامة الطيران والأمن والملاحة الجوية وإدارة المخاطر، مع الاخذ بالاعتبار للتأثيرات الاقتصادية والتشغيلية وغيرها.

وإدراكاً لطبيعة الأمن الإلكتروني متعددة الأوجه والمتعددة التخصصات والأخذ في الاعتبار أن الهجمات الإلكترونية يمكن أن تؤثر بشكل متزامن على مجموعة واسعة من المجالات وتنتشر بسرعة، فلابد من بلورة رؤية مشتركة وتطوير رؤية استراتيجية للأمن السيبراني.

وتعتمد الاستراتيجية الوطنية للأمن السيبراني للطيران المدني التابعة للهيئة العامة للطيران المدني على الاستراتيجية الوطنية للأمن السيبراني لدولة الإمارات العربية المتحدة الصادرة من قبل مجلس الأمن السيبراني لحكومة دولة الامارات واستراتيجية الأمن السيبراني للطيران التابعة لمنظمة الطيران المدني الدولي (الإيكاو).

2. الغرض من استراتيجية الأمن السيبراني الوطنية في دولة الإمارات العربية المتحدة

يهدف وجود استراتيجية وطنية للأمن السيبراني في دولة الإمارات العربية المتحدة إلى حماية البنية التحتية الحيوية وأصول المعلومات في الدولة من التهديدات والمخاطر السيبرانية. تُعد صناعة الطيران أحد القطاعات الرئيسية التي تساهم في الناتج المحلي الإجمالي والتنويع الاقتصادي لدولة الإمارات العربية المتحدة، وبالتالي تتطلب مستوى عالٍ من المرونة والأمن السيبراني. تتماشى استراتيجية الأمن السيبراني الوطنية مع توجيهات مجلس الأمن السيبراني ومنظمة الطيران المدني الدولي،

يتمثل الغرض من استراتيجية الأمن السيبراني الوطنية في دولة الامارات العربية المتحدة في حماية البنية التحتية الحيوية واصول المعلومات في الدولة من التهديدات والمخاطر السيبرانية. يعتبر قطاع الطيران أحد القطاعات الرئيسية التي تسهم في الناتج المحلي الإجمالي وتنويع الاقتصاد في دولة الامارات، وبالتالي يتطلب مستوى عالي من المقاومة والأمان السيبراني. تتماشى الإستراتيجية الوطنية للأمن السيبراني مع التوجهات من قبل مجلس الأمن السيبراني لحكومة دولة الامارات ومنظمة الطيران المدني الدولي (الإيكاو) التي توفر المعايير وأفضل الممارسات لتعزيز الأمن السيبراني لقطاع الطيران، تهدف الاستراتيجية الى تحقيق أربعة أهداف رئيسية وهي:

- إنشاء إطار حوكمة قوي للأمن السيبراني.
- تطوير قدرات ومهارات القوى العاملة في مجال الأمن السيبراني.
- تعزيز ثقافة الوعي والمسؤولية السيبرانية بين جميع أصحاب المصلحة.
- تعزيز التعاون والتنسيق بين الشركاء على المستوى الوطني والدولي في الاستجابة للحوادث والتحديات السيبرانية.

3. إدارة مخاطر الأمن السيبراني للطيران

يجب أن تتضمن إدارة مخاطر الأمن السيبراني ما يلي:

(1) الاستفادة من أطر إدارة مخاطر سلامة وأمن الطيران من أجل تطوير تقييم متكامل ودقيق لتهديدات ومخاطر الأمن السيبراني، وضمان تطوير وتنفيذ تدابير تخفيف فعالة تأخذ في الاعتبار متطلبات السلامة وتداعيات تدابير التخفيف على السلامة والأمن واستمرارية الطيران المدني.
(2) إدراك أن أحداث الأمن السيبراني التي تؤثر على سلامة الطيران المدني ليست جميعها غير قانونية و/أو مقصودة، وهناك حاجة إلى تحديد ملكية البيانات والأنظمة في جميع الأوقات. كما ينبغي للمالكين وضع القواعد والعمليات لتشمل المواقع الفعلية للبيانات والأنظمة وحقوق الوصول وأدارتها، ومتطلبات الأمان بناءً على البيانات وتصنيف النظام. وسيدعم ذلك الاستخدام المناسب للبيانات والأنظمة من قبل الأشخاص المخول لهم، ووضع وتنفيذ معايير مراقبة الجودة، وحل المشكلات والصراعات.
(3) النظر في الحاجة إلى العمل بشكل تعاوني على إطار فعال وشامل لمعالجة الأمن السيبراني للطيران المدني.
(4) دعم الأمن السيبراني والمرونة السيبرانية لنظام الطيران في مواجهة التهديدات السيبرانية التي قد تعرض سلامة أو أمن الطيران المدني للخطر.

4. مجلس الأمن السيبراني لحكومة دولة الامارات:

أعتمد مجلس الوزراء بدولة الامارات العربية المتحدة في نوفمبر 2020 إنشاء مجلس الأمن السيبراني لحكومة الامارات بهدف تطوير إسترتيجية شاملة للأمن السيبراني وإنشاء بنية تحتية سيبرانية آمنة وقوية في دولة الإمارات، وتم توقيع مذكرة تفاهم بشأن الأمن السيبراني للطيران بين شؤون مجلس الوزراء في دولة الإمارات العربية المتحدة ومنظمة الطيران المدني الدولي (الإيكاو) في مارس 2022م بهدف تعزيز الشراكة بين الإيكاو ودولة الإمارات العربية المتحدة من أجل التطوير المؤسسي وتبادل الخبرات. وسيشهد تعاونًا مكثفًا بين الطرفين وتبادل معارفهما وخبراتهما فيما يتعلق بالمسرعات والابتكار في مجال الطيران المدني المستقبلي والأمن السيبراني.

أنشأت الحكومة مجلس الأمن السيبراني ليكون هيكلاً مركزياً للأمن السيبراني على المستوى الوطني، ويتولى بالاضافة الى أمور أخرى المسؤوليات التالية:

(أ) تقديم المشورة والخبرات في مجال الأمن السيبراني .
(ب) العمل بالتعاون مع جميع الكيانات والصناعات والشركاء الأكاديميين والدوليين المعنيين لضمان أمن وأمان الفضاء الإلكتروني في الدولة.
(ج) تحليل وتقييم وكشف التهديدات والمخاطر السيبرانية .
(د) إدارة الحوادث السيبرانية الوطنية .
(هـ) دعم وتقديم المشورة للدوائر الحكومية والإدارات والجهات التنظيمية والسلطات والقطاعات والشركات .
(و) توفير الخبرة في مجال الأمن السيبراني لمساعدة ودعم جهود الحكومة في تعزيز الابتكار .
(ز) دعم صناعة الأمن السيبراني وتحفيز تطوير مهارات الأمن السيبراني .
(ح) تقديم المشورة بشأن الأمن المادي وأمن الموظفين، والذي يشكل جزءًا من نهج متعدد الطبقات لإدارة مخاطر الأمن السيبراني.

5. الاستراتيجية الوطنية للأمن السيبراني لدولة الإمارات العربية المتحدة:

تم تطوير استراتيجية الأمن السيبراني الوطنية للإمارات برؤية من مجلس الأمن السيبراني لحكومة دولة الامارات ، وتهدف الى إنشاء بنية تحتية سيبرانية آمنة ومتينة تمكن المواطنين من تحقيق تطلعاتهم وتمكين الشركات من الازدهار السيبراني في دولة الامارات العربية المتحدة، ومن الطموحات الاستراتيجية:

تتمثل تطلعات الاستراتيجية في:
(1) توفير الثقة للمواطنين للمشاركة الآمنة في العالم الرقمي .
(2) بناء قوة عاملة عالمية المستوى في مجال الأمن السيبراني في دولة الإمارات العربية المتحدة.
(3) الاحتفاء بالمساهمات في الابتكار في مجال الأمن السيبراني .
(4) تمكين الشركات الصغيرة والمتوسطة من حماية نفسها من الهجمات الإلكترونية الأكثر شيوعًا.
(5) تعزيز ثقافة ريادة الأعمال في مجال الأمن السيبراني.
(6) حماية أصول البنية التحتية للمعلومات الهامة في الدولة.

ولتحقيق هذه الطموحات، تعمل دولة الإمارات على تنفيذ عدد من المبادرات مبنية على خمسة ركائز أساسية وهي:

1. قوانين ولوائح الأمن السيبراني:
(أ) معالجة جميع أنواع الجرائم الإلكترونية.
(ب) تأمين التقنيات الحالية والناشئة .
(ج) دعم حماية الشركات الصغيرة والمتوسطة.

2. نظام بيئي نشط للأمن السيبراني:
(أ) دعم الشركات الناشئة وتعزيز البحث والتطوير في مجال الأمن السيبراني.
(ب) تطوير قدرات الأمن السيبراني .
(ج) نشر الوعي بالأمن السيبراني بين السكان.
(د) تشجيع التميز في مجال الأمن السيبراني.

3. خطة وطنية للاستجابة للحوادث:
(أ) نقطة اتصال مركزية لضحايا الحوادث السيبرانية.
(ب) خطة موحدة لتقييم الخطورة وتعبئة الجهات.
(ت) تبادل المعلومات بين الجهات.

4. برنامج حماية معلومات البنية التحتية الحيوية:
(أ) تحديد الأصول الحيوية في دولة الإمارات العربية المتحدة .
(ب) وضع معايير عالمية المستوى لإدارة المخاطر .
(ج) إنشاء عمليات قوية للإبلاغ والامتثال والاستجابة.

5. شراكات:
(أ) اللجان الوطنية.
(ب) الشراكات المحلية .
(ج) الشراكات العالمية.

6. استراتيجية الأمن الالكتروني في مجال الطيران لمنظمة الطيران المدني الدولي:

تتمثل رؤية منظمة الطيران المدني الدولي للأمن السيبراني العالمية في أن يكون قطاع الطيران المدني مرنًا في مواجهة الهجمات الإلكترونية ويظل آمنًا وموثوقًا به مع الاستمرار في الابتكار والنمو على مستوى العالم. وتتوافق استراتيجية الأمن السيبراني للطيران مع مبادرات منظمة الطيران المدني الدولي الأخرى المتعلقة بالإنترنت بالتنسيق مع أحكام إدارة سلامة الطيران وأمن الطيران المقابلة.

ويتم تحقيق أهداف الاستراتيجية من خلال سلسلة من المبادئ والتدابير والإجراءات الواردة في إطار عمل مبني على سبع ركائز رئيسية، وهي كالتالي:

(1) التعاون الدولي.
(2) النظم الادارية .
(3) التشريعات واللوائح الفعالة.
(4) السياسات المرتبطة بالأمن الإلكتروني.
(5) تبادل المعلومات.
(6) إدارة الوقائع والتخطيط للطوارئ.
(7) بناء القدرات والتدريب وترسيخ ثقافة الأمن الألكتروني.

7. رؤية الهيئة العامة للطيران المدني الوطنية للأمن السيبراني للطيران:

رؤية الهيئة العامة للطيران المدني الوطنية للأمن السيبراني للطيران هيالحفاظ على قطاع الطيران المدني في دولة الإمارات العربية المتحدة بأمن وأمان وموثوقية واستدامة وقدرة على الصمود ضد مواجهة الهجمات الإلكترونية.

ويمكن تحقيق ذلك من خلال:

(أ) الاعتراف بالالتزامات بموجب اتفاقية الطيران المدني الدولي (اتفاقية شيكاغو) لضمان سلامة وأمن واستمرارية الطيران المدني، مع مراعاة الأمن السيبراني.
(ب) الاعتراف بمبادرة إعلان دبي بشأن الأمن السيبراني في مجال الطيران المدني، وقرار الدورة الاربعون لجمعية الايكاو العمومية رقم (10) الذي يؤكد من جديد على أهمية معالجة الأمن السيبراني والمرونة السيبرانية للأنظمة والبيانات والمعلومات الهامة للطيران المدني ضد التهديدات والمخاطر الإلكترونية.
(ج) تنسيق الأمن السيبراني للطيران بين السلطات الوطنية المعنية لضمان الإدارة الفعالة والكفاءة لمخاطر الأمن السيبراني.
(د) التزام أصحاب المصلحة في مجال الطيران المدني في دولة الإمارات العربية المتحدة بمواصلة تطوير المرونة السيبرانية، والحماية ضد الهجمات الإلكترونية التي قد تؤثر على سلامة وأمن واستمرارية أنظمة النقل الجوي.

8. الاستراتيجية العامة للهيئة العامة للطيران المدني:

تحدد الأهداف الاستراتيجية للهيئة العامة للطيران المدني التوجه طويل المدى لوضع سياسات الطيران لعام 2050 وما بعدها:

(1) تطوير وإنفاذ لوائح السلامة والأمن وفقًا للمعايير الدولية وأفضل الممارسات .
(2) التحسينات المستمرة لمعايير السلامة والخدمة في تقديم خدمات الملاحة الجوية .
(3) الارتقاء بقطاع الطيران الإماراتي في المحافل العالمية .
(4) التحسينات المستمرة في العلاقات الثنائية .
(5) ضمان تقديم خدمات الهيئة العامة للطيران المدني وفقًا لمعايير الجودة والكفاءة والشفافية.
(6) غرس ثقافة الابتكار في بيئة العمل المؤسسية.

ستساهم الإستراتيجية الوطنية للأمن السيبراني للطيران المدني للهيئة العامة للطيران المدني بشكل مباشر في تحقيق الهدف رقم 1 المذكور أعلاه. كما ستسهل تحقيق الأهداف 2 و3 و6 من خلال دعم تطوير البيئة التنظيمية والتقدم التكنولوجي.

9. فريق عمل الهيئة العامة للطيران المدني للأمن السيبراني لقطاع الطيران المدني:

يهدف فريق عمل الأمن السيبراني التابع للهيئة العامة للطيران المدني إلى أن تضع منظومة الطيران المدني تدابير تخفيف متينة ومرنة وديناميكية للحد من المخاطر السيبرانية المحتملة، مدعومة بنظام إشراف تنظيمي متناسب متفق عليه. سيمكن ذلك جميع أصحاب المصلحة في مجال صناعة الطيران من استغلال فوائد الفضاء الإلكتروني دون المساس بأمن وسلامة الطيران والملاحة الجوية واستمرارية الخدمات.

1.9 أهداف استراتيجية الأمن السيبراني الوطني للطيران المدني للهيئة العامة للطيران المدني:

1.1.9 أهداف الإستراتيجية الوطنية للأمن السيبراني للطيران المدني هي:

(1) تعزيز ثقافة الأمن السيبراني في مجال الطيران المدني .
(2) تمكين أصحاب المصلحة في مجال الطيران المدني من حماية أنفسهم من الهجمات السيبرانية الشائعة .
(3) مطالبة أصحاب المصلحة بتحديد وحماية أنظمة وتقنيات المعلومات والاتصالات والبيانات الهامة الحرجة المستخدمة لأغراض الطيران المدني، بما في ذلك البنية التحتية وأصول الدولة.
(4) تطوير موارد بشرية وقدرات وكفاءات كافية من خلال تقديم تدريب مناسب ومتماسك وذي صلة بالأمن السيبراني للطيران لموظفي السلطة المختصة للطيران المدني وأصحاب المصلحة المعنيين في منظومة الطيران المدني.
(5) ضمان استمرارية الأعمال المتعلقة بالأمن السيبراني .
(6) توفير الثقة لأصحاب المصلحة في مجال الطيران والجمهور والمسافرين للمشاركة الآمنة في العالم الرقمي.
(7) المساهمة في الابتكار في مجال الأمن السيبراني.

2.1.9 لتحقيق الأهداف المذكورة من خلال هذه الاستراتيجية، فإن المبادئ الشاملة هي:
(أ) فهم المخاطر التي تشكلها التهديدات السيبرانية ونقاط الضعف داخل قطاع الطيران، وعواقبها المحتملة.
(ب) إدارة المخاطر السيبرانية واتخاذ الإجراءات المناسبة والمتناسبة لحماية الأصول الرئيسية.
(ج) الاستجابة للأحداث والحوادث الإلكترونية والتعافي منها بشكل فعال وضمان تعلم الدروس.
(د) تعزيز التغييرات الثقافية وزيادة الوعي وبناء القدرات الإلكترونية.

10. ركائز استراتيجية الأمن السيبراني الوطني للطيران المدني للهيئة العامة للطيران المدني:

تتماشى استراتيجية الأمن السيبراني الوطني للطيران المدني للهيئة العامة للطيران المدني مع ركائز الأمن السيبراني الوطنية لدولة الإمارات العربية المتحدة ومبادرات وركائز منظمة الطيران المدني الدولي (الايكاو) المعنية بأحكام إدارة أمن وسلامة الطيران المدني. وسيتم تحقيق هذه الاستراتيجية من خلال سلسلة من المبادئ والتدابير والإجراءات الواردة في إطار عمل مبني على سبع ركائز وهي:

(1) التعاون الدولي والشراكة.
(2) الحوكمة.
(3) التشريعات واللوائح الفعالة.

(4) سياسة الأمن الإلكتروني.
(5) تبادل المعلومات.
(6) إدارة الوقائع والتخطيط للطوارئ.
(7) بناء القدرات والتدريب وترسيخ ثقافة الأمن الألكتروني.

1. التعاون الدولي والشراكة

(1) تدعم الهيئة العامة للطيران المدني مواءمة الأمن السيبراني للطيران على المستويات العالمية والإقليمية والوطنية من أجل ضمان الاتساق وقابلية التشغيل البيني الكاملة ونظام إدارة المخاطر، إن الأمن السيبراني والطيران كلاهما بطبيعتهما بلا حدود. ويجب على الهيئة العامة للطيران المدني دعم التعاون على المستويين الوطني والدولي والدعوة إلى الاعتراف المتبادل بالجهود المبذولة لتطوير الأمن السيبراني والحفاظ عليه وتحسينه بهدف حماية قطاع الطيران المدني من جميع التهديدات الإلكترونية للسلامة والأمن.
(2) ستدعم الهيئة العامة للطيران المدني تطوير شراكات فعالة مع القطاعين العام والخاص حسب الحاجة.

2. الحوكمة

(1) وضع حوكمة وطنية واضحة ومسئوليات وفقًا لمتطلبات مجلس الأمن السيبراني لحكومة دولة الامارات بالتزامن مع خطة عمل الأمن السيبراني لمنظمة الطيران المدني الدولي. (الايكاو).
(2) وضع حوكمة وطنية واضحة للأمن السيبراني للطيران المدني من خلال تعيين الهيئة العامة للطيران المدني كسلطة مختصة للأمن السيبراني للطيران المدني في دولة الإمارات العربية المتحدة مع صلاحيات شاملة ومسؤولية عن الأمن السيبراني للطيران والمرونة السيبرانية.
(3) تحديد الأدوار والمسؤوليات التي ستضطلع بها الكيانات وأصحاب المصلحة المعنيين فيما يتعلق بالأمن السيبراني للطيران المدني.
(4) يجب على السلطة المختصة المختصة للأمن السيبراني للطيران ضمان التنسيق مع أصحاب المصلحة المعنيين في مجال الطيران المدني والأمن السيبراني من خلال إنشاء قنوات تنسيق مناسبة.
(5) يجب أن تكون استراتيجية الأمن السيبراني الوطني للطيران في الهيئة العامة للطيران المدني هي الأساس للشركاء لتطوير استراتيجيات الأمن السيبراني للطيران المدني الخاصة بهم لضمان أمن وسلامة واستمرارية الطيران المدني في بيئة تتعرض للخطر بسبب التهديدات السيبرانية.

3. التشريعات واللوائح الفعالة

(1) ضمان أن تكون التشريعات واللوائح المناسبة مبنية على أحكام منظمة الطيران المدني الدولي ويتم صيانتها وفقًا لذلك. مواصلة تطوير التوجيهات المناسبة لأصحاب المصلحة والصناعة في تنفيذ الأحكام المتعلقة بالأمن السيبراني. تلتزم الهيئة العامة للطيران المدني بإنشاء ومراجعة وتعديل، حسب الاقتضاء، المواد الإرشادية المتعلقة بإدراج جوانب الأمن السيبراني في الأمن والسلامة.
(2) دعم تطوير وتنفيذ استراتيجية الأمن السيبراني الشاملة هذه لحماية الطيران المدني والجمهور المسافر من آثار الهجمات الإلكترونية من خلال تطوير تشريعات ولوائح الأمن السيبراني للطيران المتوافقة على المستويات الدولي والإقليمي والوطني.
(3) دعم تطوير الصكوك القانونية الدولية ذات الصلة التي تتناول الأحكام القانونية الرئيسية لمنع ومقاضاة ورد الفعل في الوقت المناسب على الحوادث الإلكترونية من أجل تشكيل الأساس للتنفيذ المتسق والمتماسك لتشريعات ولوائح الأمن السيبراني في جميع أنحاء قطاع الطيران العالمي.
(4) دعم المزيد من تطوير التشريعات الوطنية لمقاضاة التهديدات الإلكترونية المتطورة المتعلقة بالإرهاب بالإضافة إلى الهجمات الإلكترونية التي تؤثر على الطيران المدني.
(5) تضمين أحكام بشأن الأمن السيبراني للطيران في برامج الأمن والسلامة الوطنية للطيران المدني وفقًا لمعايير ولوائح منظمة الطيران المدني الدولي.

4. سياسة الأمن السيبراني

(1) دعم وتشجيع تطوير سياسات الأمن السيبراني مثل: ثقافة الأمن السيبراني، وتعزيز الأمن من خلال التصميم، وأمن سلسلة التوريد للبرامج والأجهزة، وسلامة البيانات، والتحكم المناسب في الوصول، وإدارة الثغرات الأمنية الاستباقية، وتحسين المرونة في تحديثات الأمان دون المساس بالسلامة، بالإضافة إلى دمج الأنظمة والعمليات لمراقبة بيانات الأمن السيبراني ذات الصلة.

(2) تضمين الأمن السيبراني ضمن أنظمة الإشراف على أمن وسلامة الطيران في الهيئة العامة للطيران المدني كجزء من إطار عمل شامل لإدارة المخاطر.

(3) مواصلة تطوير المواد الإرشادية المتعلقة بتقييمات التهديدات والمخاطر السيبرانية بهدف تحقيق قابلية المقارنة لنتائج هذه التقييمات مع مراعاة منهجيات تقييم المخاطر المختلفة.

(4) التوافق مع سياسة حماية البنية التحتية للمعلومات الهامة والحرجة الصادرة عن مجلس الأمن السيبراني لحكومة دولة الامارات.

5. تبادل المعلومات

(1) دعم ثقافة تبادل المعلومات للسماح بالوقاية والكشف المبكر والتخفيف من أحداث الأمن السيبراني ذات الصلة قبل أن تؤدي إلى آثار أوسع على أمن أو سلامة الطيران. تقليل المخاطر السيبرانية النظامية عبر قطاع الطيران من خلال تنفيذ ثقافة تبادل المعلومات التي تم إثبات قيمتها بالفعل عبر أمن وسلامة الطيران.

(2) تقليل تأثير الهجمات المستمرة من خلال تبادل المعلومات حول جوانب مثل نقاط الضعف والتهديدات والأحداث وأفضل الممارسات، وذلك خلال قنوات ثابتة وموثوقة بما يتماشى مع أحكام منظمة الطيران المدني الدولي (الايكاو).

6. إدارة الوقائع والتخطيط للطوارئ

(1) تنسيق إدارة الحوادث والتخطيط للطوارئ مع مجلس الأمن السيبراني لحكومة دولة الامارات لتلبية متطلبات الأمن السيبراني الوطنية.

(2) ضمان استمرارية النقل الجوي أثناء الحوادث السيبرانية من خلال تضمين خطط الأمن السيبراني المناسبة والقابلة للتطوير في آليات إدارة الحوادث الحالية. تعديل خطط الطوارئ الحالية لتشمل أحكامًا للأمن السيبراني.

(3) تشجيع إجراء تمارين الأمن السيبراني (تمارين المحاكاة على الطاولة أو عمليات المحاكاة أو التمارين في الوقت الفعلي)، وهي أداة مفيدة لاختبار المرونة السيبرانية وتحديد التحسينات.

7. بناء القدرات والتدريب وترسيخ ثقافة الأمن السيبراني

(1) زيادة عدد الموظفين المؤهلين وذوي المعرفة في كل من الطيران والأمن السيبراني لأن العنصر البشري أمر بالغ الأهمية بالإضافة إلى كونه جوهر الأمن السيبراني. تعزيز الوعي بالأمن السيبراني، بالإضافة إلى التعليم والتوظيف والتدريب. تضمين مناهج الأمن السيبراني ذات الصلة في إطار التعليم الوطني وبرامج التدريب، وحيثما يكون ذلك عمليًا، تضمين الأمن السيبراني الخاص بالطيران على جميع المستويات.

(2) دعم وتحفيز تطوير المهارات في القوى العاملة الحالية والجديدة لتمكين تعزيز الابتكار في مجال الأمن السيبراني والبحث والتصميم المناسبين في قطاع الطيران. ضمان التدريب المناسب المتعلق بالوظيفة بشكل مستمر لدعم الموظفين في أدوارهم اليومية.

(3) تضمين الأمن السيبراني في استراتيجية الجيل القادم من متخصصي الطيران بناءً على مبادرات منظمة الطيران المدني الدولي لتطوير متطلبات الكفاءة القائمة على الأدوار لمتخصصي الطيران.

(4) تطبيق مبادئ ثقافة الأمن والسلامة الاستباقية لتطوير ثقافة الأمن السيبراني والحفاظ عليها في جميع أنحاء قطاع الطيران، مما يجعلها مسؤولية الجميع.

- إنتهى -