سياسة الأمن السيبراني في الطيران المدني لدولة الإمارات العربية المتحدة

١. المقدمة

١,١ تعتبر سياسة الأمن السيبراني إطاراً لمواصلة تطوير وتنفيذ الأمن السيبراني في مجال الطيران المدني في دولة الإمارات العربية المتحدة، وسيجري نشرها وتوزيعها على الجهات المعنية ومراجعتها بشكل دوري.

٢,١ يجب تطوير المزيد من المواد الإسترشادية من أجل دعم تنفيذ سياسة الأمن السيبراني هذه في مجال الطيران المدني.

٢. النطاق

١,٢ يجب أن يتناول الأمن السيبراني في الطيران المدني أمن ومتانة نظام الطيران المدني، بالإضافة إلى دعم التعاون مع السلطات والجهات من خارج قطاع الطيران، بما في ذلك مجلس الأمن السيبراني لحكومة دولة الإمارات العربية المتحدة، وجهاز أمن الدولة، و وزارة الداخلية، و وزارة الدفاع حسب الاقتضاء.

٢,٢ يجب تنسيق الأمن السيبراني في مجال الطيران المدني على المستوى الوطني مع سلامة الطيران، وأمن الطيران، وحماية البنية الاساسية الحيوية، وشبكة الدفاع السيبرانية والجيش.

٣,٢ يجب تنسيق الأمن السيبراني في الطيران المدني على الصعيد الدولي مع الجهات والسلطات الأجنبية المعنية بالأمن السيبراني في مجال الطيران المدني.

٣. الأهداف

١,٣ تتمثل الأهداف العامة لسياسة الأمن السيبراني في الطيران المدني ضمان أمن منظومة الطيران المدني وقدرتها على الصمود في وجه التهديدات والهجمات السيبرانية، وضمان تنسيق الأمن السيبراني في الطيران المدني مع السلطات والكيانات الوطنية المعنية.

٤. الحوكمة والتنظيم

١,٤ وفقًا لرسالة وزارة الاقتصاد لدولة الإمارات العربية المتحدة المرجع GCAA/C/٥٤-٢٣ بتاريخ ٣١ أكتوبر ٢٠٢٣ من معالي وزير الاقتصاد ورئيس مجلس إدارة الهيئة العامة للطيران المدني إلى منظمة الطيران المدني الدولية (الإيكاو)، تم تعيين الهيئة العامة للطيران المدني كسلطة معنية بالأمن السيبراني للطيران بصلاحيات عامة للأمن السيبراني في الطيران المدني والصمود السيبراني.

٢,٤ يجب على الهيئة العامة للطيران المدني:

أ. تحديد، بالتنسيق مع السلطة الوطنية المختصة للأمن السيبراني (مجلس الأمن السيبراني لحكومة دولة الامارات العربية المتحدة)، الأدوار والمسؤوليات التي يجب أن تضطلع بها كل سلطة وكيان في الإمارات والمتصلة بالأمن السيبراني في الطيران المدني والصمود السيبراني.

ب. قيادة تطوير لوائح الأمن السيبراني في الطيران المدني.

ج. تحديد الأدوار والمسؤوليات للقطاعات داخل الهيئة العامة للطيران المدني المتعلقة بالأمن السيبراني.

د. تنسيق وتحديد الأدوار والمسؤوليات للكيانات في الطيران المدني التي تشرف عليها الهيئة العامة للطيران المدني من خلال البرنامج الوطني للسلامة والبرنامج الوطني لأمن الطيران المدني.

هـ. تحديد عناصر ثقافة الأمن السيبراني في الطيران المدني ورصد تنفيذها.

و. تحديد اللوائح والعمليات والاجرءات والمتطلبات والأدوار لإدارة الأزمات السيبرانية في الطيران المدني، بما في ذلك متطلبات الاختبار والتواتر.

ز. تنسيق القضايا السيبرانية في الطيران المدني مع الجهات خارج الطيران المدني ذات الصلة المشاركة في الأمن السيبراني في الطيران المدني مثل تبادل المعلومات وتحقيق الحوادث.

ح. تمثيل دولة الإمارات العربية المتحدة في المنتديات ذات الصلة بالأمن السيبراني في الطيران على الصعيدين الدولي والإقليمي والثنائي، بما في ذلك على سبيل المثال لا الحصر منظمة الطيران المدني الدولية (الإيكاو) للأمن السيبراني، ولجان العمل والفرق التابعة لها، وما إلى ذلك حسب الاقتضاء.

ط. تنفيذ أدوار ومسؤوليات أخرى وفقًا لمعايير منظمة الطيران المدني الدولية (الإيكاو) والممارسات الموصى بها، فضلاً عن الكيانات الدولية المعنية الأخرى في مجال السلامة الدولية للطيران وأمن الطيران، حسب الاقتضاء.

٥. إدارة المخاطر

١,٥ يجب أن يكون الأمن السيبراني مدفوعًا بقدرات استخبارية، وقائماً على التهديد، وأن تطبق فيه منهجية إدارة المخاطر.

٢,٥ يجب أن تكون إدارة المخاطر جزءًا لا يتجزأ من دورة حياة المنظومة الشاملة.

٣,٥ يجب أن تكون ملكية جميع البيانات والنظم محددة في جميع الاوقات.

٦. أمن النظم الحرجة

١,٦ يجب تحديد الوظائف والأنظمة والبنية الاساسية الحيوية في عمليات إدارة المخاطر.

٢,٦ يجب تطبيق نهج "الأمن بفضل التصميم" مقترناً بمبادئ "الدفاع العميق" من أجل حماية الأنظمة الحرجة.

٣,٦ يجب إعتبار تكرار الأنظمة الحيوية بمثابة عامل تمكين لأمن النظام والتوافر المستمر والمرونة التشغيلية ضد حالات الفشل الناجمة عن التهديدات السيبرانية.

٤,٦ لتحقيق والحفاظ على الحماية المناسبة للأصول التنظيمية، يجب أن يتم حساب جميع الأصول وأن يكون لكل منها مالك محدد.

٧. أمن البيانات

١,٧ يجب حماية البيانات والمعلومات أثناء التخزين والارسال، بما يتماشى مع حساسيتها.

٢,٧ يجب التحكم في الوصول إلى المعلومات ومرافق معالجة المعلومات والعمليات على أساس متطلبات الأعمال والأمن.

٨. أمن سلسلة التوريد

١,٨ يجب أن يكون إدارة سلسلة التوريد من البرمجيات/الأجهزة نهايةً إلى نهاية جزءًا من إدارة الأمن السيبراني للطيران المدني.

٢,٨ يجب أن تتوافق البرمجيات والأجهزة المستخدمة في الوظائف الطيرانية الحيوية مع متطلبات الأمن السيبراني طوال دورة حياة الأنظمة الطيرانية.

٩. الأمن المادي

١,٩ يجب أن يكون الأمن المادي (بما في ذلك أمن الموظفين) جزءًا من إدارة الأمن السيبراني في مجال الطيران المدني.

٢,٩ يجب أن يحمي الأمن المادي الأشخاص والبنية التحتية الاساسية والمرافق والمعدات والمواد والوثائق من أي تدخل غير مشروع، وحماية نظم الطيران الحيوية من الوصول المادي غير المصرح به.

٣,٩ يجب أن يسهم الأمن المادي في إدارة المخاطر من خلال دعم تحديد الكيانات المهددة و/أو احتمال شن هجمات على البنية الاساسية الحيوية للطيران المدني.

١٠. أمن تكنولوجيا المعلومات والاتصالات (ICT)

١,١٠ يجب أن يكون أمن تكنولوجيا المعلومات والاتصالات جزءًا من إدارة الأمن السيبراني في مجال الطيران المدني.

٢,١٠ يجب أن يحدد أمن تكنولوجيا المعلومات والاتصالات تدابير أمن منطقية وينفذها، بالإضافة إلى المساهمة في عمليات إدارة الوقائع السيبرانية والتعافي من آثارها، وفي استمرارية التشغيل.

٣,١٠ يجب أن يساهم أمن تكنولوجيا المعلومات والاتصالات في إدارة المخاطر من خلال تحديد الثغرات ونقاط الضعف ونقاط الهجوم ورصد تطور مشهد تهديد الأمن السيبراني في مجال الطيران المدني.

١١. إدارة الوقائع واستمرارية المهام الحيوية

١,١١ المحرك الأساسي لعمليات إدارة الوقائع هو سلامة العمليات واستمرارية المهام الحيوية.

٢,١١ يجب أن يكون اختبار خطط إدارة الأزمات والتعافي من آثارها جزءًا لا يتجزأ من إدارة الوقائع.

١٢. ثقافة الأمن السيبراني

١,١٢ يجب أن تكون خطة التعليم والتوعية والتدريب والتمارين جزءًا لا يتجزأ من إدارة الأمن السيبراني في مجال الطيران المدني.

٢,١٢ يجب تنسيق ثقافة الأمن السيبراني بشكل كامل بشكل كامل مع الثقافات القائمة للأمن والسلامة.

٣,١٢ يجب أن تدعم ثقافة الأمن السيبراني بممارسات قوية لتبادل المعلومات داخلياً وبالقدر الممكن خارجياً.