إرشادات بشأن سياسة الأمن الإلكتروني

نشرت بموجب سلطة الأمين العام
يناير ٢٠٢٢
منظمة الطيران المدني الدولي

١- المُقدِّمة

تتماشى هذه الإرشادات مع استراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران١ وخطة عمل الأمن الإلكتروني٢، التي يوصي بندها الإجرائي CyAP0.1 بأن تتولى الإيكاو وضع نموذج لسياسة الأمن الإلكتروني كمرجع للدول الأعضاء وقطاع الطيران عند قيامهم بتطوير سياساتهم الوطنية/الداخلية.

وترد سياسة الأمن الإلكتروني النموذجية في المرفق (أ) بهذه الإرشادات.

٢- النطاق

يتناول نموذج سياسة الأمن الإلكتروني المُبيَّن في المرفق (أ) من هذه الوثيقة موضوع حماية البنية الأساسية الحيوية لمنظومة الطيران المدني الدولي ضد التهديدات الإلكترونية وتعزيز قدرتها على الصمود في وجه هذه التهديدات، كما يتناول مُتطلَّبات التعاون المتعدد الأطراف داخل منظومة الطيران المدني وكذلك مع السلطات الخارجية مثل الجيش والجهات المختصة بالأمن الإلكتروني والأمن القومي.

٣- الأهداف

الهدف هو أن يكون نموذج سياسة الأمن الإلكتروني بمثابة دليل لمساعدة الدول وقطاع الطيران على تركيز الموارد والإجراءات لتحقيق نهج نظامي للأمن الإلكتروني في مجال الطيران المدني، بما في ذلك النظم الحالية والموروثة. والهدف النهائي هو تمكين الدول والأطراف المعنية من وضع نهج لنظام النُظُم يُمكِّن من حماية الطيران المدني من التهديدات الإلكترونية، والاستجابة للوقائع الإلكترونية والتعافي منها في الوقت المناسب، وبالتالي التمكُّن من الصمود في وجه التهديدات الجديدة دون حدوث اضطرابات كبيرة.

وفيما يلي النتائج الرئيسية المتوقَّعة من تنفيذ سياسة الأمن الإلكتروني:

٣-١ ضمان حماية الطيران المدني من التهديدات الإلكترونية

تجري معالجة مسألة حماية الطيران المدني من الهجمات الإلكترونية من خلال تنفيذ قواعد الإيكاو وتوصياتها الدولية وإجراءاتها وإرشاداتها في ما يتعلَّق بالأمن الإلكتروني. ويشمل ذلك تنفيذ ممارسات قوية لإدارة المخاطر، وتحديد البنية الأساسية الحيوية، وتنفيذ نهج شامل متعدد المستويات للأمن الإلكتروني. وينبغي أن يضمن هذا النهج ألا يتسبب نجاح الهجوم على مستوى واحد في تعرُّض بقية المستويات الأخرى من النظام للخطر و/أو في فقدان السلامة أو الأمن أو استمرارية الوظائف الحيوية. كما ينبغي للنظام أن يعتمد نهجاً للتحسين المستمر لضمان تنسيق التحسينات اللازمة للتطورات التقنية أو الإجرائية المخطط لها وتنفيذها والمواظبة على تحديثها.

٣-٢ ضمان قدرة الطيران المدني على الصمود أمام التهديدات الإلكترونية

نظام الطيران المدني القادر على الصمود أمام التهديدات الإلكترونية هو نظام قادرٌ على الحفاظ على أداء وظائفه الحيوية تحت الهجمات: أيّ، تمكُّن النظام من دعم سلامة وأمن عمليات الطيران بأقل قدر ممكن من التعطيل، إن وجد. وينبغي أن يشمل النظام أيضاً آليات مناسبة للتعاون وتبادل المعلومات بين أصحاب المصلحة في مجال الطيران، مثل الحكومة وقطاع الطيران، وعند الاقتضاء، مع سلطات إنفاذ القانون المدني والسلطات العسكرية.

٣-٣ ضمان قدرة الطيران المدني على حماية ذاته باعتماد نهج "الأمن بفضل التصميم"

يتطلب اعتماد نهج "الأمن بفضل التصميم" للطيران المدني، في بداية تصوُّر النظام، النظر في الأهداف الأمنية التي يجب تحقيقها أثناء عملية تصميم النظام، إلى جانب الأهداف التقليدية المتعلقة بالتشغيل والسلامة. ويؤدي ضمان أمن العناصر

---

١ https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

٢ كتاب المنظمة SL 2020/114

والعمليات الحاسمة "بفضل التصميم" إلى تغيير النموذج الأمني من الأسلوب القائم على ردة الفعل إلى الأسلوب الاستباقي، وإلى تطوير نظام للطيران المدني يتمتع بالحماية الذاتية، مما يمكنه من التطور ومن تحسين الأمن والقدرة على تحمل التهديدات.

٤-٣ ضمان تنسيق الأمن الإلكتروني في مجال الطيران المدني مع أصحاب المصلحة المعنيين من خارج قطاع الطيران

من أجل ضمان اتباع نهج متسق ومكمِّل للأمن الإلكتروني في مجال الطيران على نطاق تخصصات الطيران، يجب أن يضمن نظام الطيران المدني توفير الإدارة الشاملة للمخاطر الإلكترونية على الطيران المدني من خلال تنسيق جوانب السلامة والأمن المُتعلِّقة بالأمن الإلكتروني في مجال الطيران. وبالإضافة إلى ذلك، ينبغي أن يمتد تنسيق الأمن الإلكتروني في مجال الطيران إلى خارج قطاع الطيران المدني ليشمل الكيانات المعنية الأخرى مثل السلطات الوطنية/الإقليمية/الدولية المختصة بالأمن الإلكتروني وإنفاذ القانون والجيش وما إلى ذلك.

٤- عناصر سياسة الأمن الإلكتروني

يقدِّم هذا القسم إرشادات بشأن العناصر المُتضمَّنة في نموذج سياسة الأمن الإلكتروني الوارد في المرفق (أ). وبالتالي، فمن المستصوب قراءته مع نموذج سياسة الأمن الإلكتروني.

٤-١ أساليب الإدارة والتنظيم

٤-١-١ ينبغي للدول أن تعيِّن سلطة مختصَّة بالأمن الإلكتروني في مجال الطيران (AA/Cyber)، مع منحها ولاية ومسؤولية شاملتين عن الأمن الإلكتروني في مجال الطيران والصمود أمام التهديدات الإلكترونية.

٤-١-٢ لا يوجد حل أو نموذج واحد يناسب الجميع في ما يتعلق بموقع السلطة المختصَّة بالأمن الإلكتروني في مجال الطيران لكل بلد ضمن هيكلها التنظيمي للطيران المدني. إذ إن القرار يتأثر بعدة اعتبارات تتعلق بمنظومة الطيران الوطنية والبيئة ذات الصلة من خارج قطاع الطيران من حيث الكيانات والولايات. بيد أنه من المهم تزويد السلطة المختصَّة بالأمن الإلكتروني في مجال الطيران بما يلزم من الموارد والسلطة لتمكينها من الاضطلاع بولايتها، بما في ذلك سلطة التفاوض والتنسيق مع أصحاب المصلحة المعنيين من خارج قطاع الطيران.

٤-١-٣ وبشكل عام، ينبغي للسلطة المختصَّة بالأمن الإلكتروني في مجال الطيران القيام بما يلي:

- التنسيق مع السلطة الوطنية المختصة بالأمن الإلكتروني من أجل تحديد أدوار ومسؤوليات كل سلطة منهما؛
- قيادة تطوير لوائح الأمن الإلكتروني في مجال الطيران؛
- التحديد بوضوح للأدوار والمسؤوليات لمختلف مجالات الطيران المدني داخل السلطة الوطنية المختصة بالطيران المدني؛
- تنسيق عملية تحديد أدوار ومسؤوليات هيئات الطيران المدني التي تشرف عليها السلطة الوطنية المختصة بالطيران المدني من خلال البرامج الوطنية للسلامة والأمن؛
- تحديد عناصر ثقافة الأمن الإلكتروني في مجال الطيران المدني ورصد تنفيذها؛
- تحديد اللوائح والعمليات والمُتطلَّبات والأدوار المُتعلِّقة بإدارة أزمات الأمن الإلكتروني، بما في ذلك متطلبات الاختبار ووتيرته؛
- تنسيق القضايا المتشعبة المُتعلِّقة بالأمن الإلكتروني في مجال الطيران مع أصحاب المصلحة من خارج قطاع الطيران من المعنيين بالأمن الإلكتروني في مجال الطيران مثل تبادل المعلومات والتحقيق في الوقائع.

٤-٢ إدارة المخاطر

٤-٢-١ ينبغي أن تعتمد إدارة مخاطر الأمن الإلكتروني على أطر إدارة مخاطر السلامة والأمن في مجال الطيران من أجل وضع تقييم متكامل ودقيق لتهديدات ومخاطر الأمن الإلكتروني، وضمان وضع وتنفيذ تدابير فعَّالة للتخفيف، تراعي مُتطلَّبات السلامة وآثار تدابير التخفيف على سلامة الطيران المدني واستمراريته.

٤-٢-٢ يجب أن تكون ملكية جميع البيانات والنُظُم مُحدَّدة في جميع الأوقات. إذ إن تحديد الملكية والمحافظة عليها يمهد للمساءلة ويدعم إدارة البيانات والنُظُم بدءاً من مرحلة استقبالها واستخدامها حتى مرحلة انتفاء الحاجة إليها والتخلص منها. وعلى هذا النحو، ينبغي أن يقوم مالكو البيانات والنُظُم بإنشاء قواعد وعمليات تشمل المواقع المادية للبيانات والنُظُم، وحقوق الوصول والاستخدام، وحقوق الإدارة، ومُتطلَّبات الأمن استناداً إلى تصنيف البيانات والنُظُم. وهذا يدعم في نهاية المطاف الاستخدام الملائم للبيانات والنُظُم من قبل الأشخاص المناسبين، ووضع معايير مراقبة الجودة وتنفيذها، وحل القضايا والنزاعات.

٤-٣ أمن النُظُم الحرجة

٤-٣-١ ينبغي تطبيق مبادئ "الدفاع العميق" من أجل حماية النُظُم الحرجة. فالدفاع العميق يُدمج قدرات الناس والتكنولوجيا والعمليات من أجل وضع حواجز متغيرة عبر مستويات ومهام متعددة للمنظمة[٣]. ويمثل ذلك نهجاً للأمن الإلكتروني يوظف سلسلة من الآليات الدفاعية على مستويات لحماية النُظُم والبيانات والمعلومات الهامة. ويُعزِّز هذا النهج متعدد المستويات، إلى جانب التكرار المتعمَّد، أمن النظام ككل ويتصدّى للعديد من ناقلات الهجمات المختلفة[٤].

٤-٣-٢ يجب أن تضمن السلطة المختصَّة بالأمن الإلكتروني في مجال الطيران (AA/Cyber) قيام الكيانات المعنية بالطيران المدني بتحديد أنظمتها الحيوية وحمايتها بشكلٍ كافٍ، فضلاً عن تطوير القدرة على اكتشاف الوقائع الإلكترونية والتصدِّي لها والتعافي من آثارها.

٤-٤ أمن البيانات

٤-٤-١ ينبغي مراعاة القيام دورياً بإجراء النسخ الاحتياطي الآمن دون اتصال بالإنترنت من أجل البيانات الهامة كعنصر تمكين لدعم إتاحة المعلومات وسلامتها. ومع ذلك، فمن الضروري وضع سياسة صارمة في ما يتعلَّق بالنسخ الاحتياطي، بما يتماشى مع تقييمات المخاطر، وذلك نظراً لأن إجراء النسخ الاحتياطي غير المتصل بالإنترنت في ظل وجود هجوم إلكتروني سيجعل البيانات والنُظُم مُعرَّضة للخطر بالفعل، وبالتالي لا يمكن استخدامه لاستعادة الوصول إلى المعلومات الهامة.

٤-٤-٢ ينبغي مراعاة ترميز (تشفير) البيانات الحسَّاسة كعنصر تمكين لدعم سرية المعلومات. ومع ذلك، فمن المهم تحديد عمليات استخدام التشفير، بما يتماشى مع تقييمات المخاطر، التي تحقق التوازن المناسب بين مستوى السرية ومُتطلَّبات الأداء التشغيلي، لا سيما في ما يتعلَّق بالبيانات "الحية" اللازمة لسلامة الطيران، فضلاً عن مراعاة الموارد اللازمة لإدارة البيانات.

٤-٤-٣ ينبغي إنشاء عمليات لضمان استمرارية المهام الحيوية في حالة فقدان إتاحة البيانات و/أو تقويض سلامتها.

٤-٥ أمن سلسلة التوريد

٤-٥-١ ينبغي للكيانات أن تكفل امتثال البرمجيات والأجهزة المستخدمة في وظائف الطيران الحيوية لمُتطلَّبات الأمن الإلكتروني على مدى دورة حياة نُظُم الطيران، بدءًا من التصميم والتطوير مروراً بالتشغيل والصيانة حتى التخلص منها بشكل سليم وآمن.

٤-٥-٢ يمكن الاستفادة من اتفاقات مستوى الخدمة بحيث تشمل مُتطلَّبات الأمن الإلكتروني للأجهزة والبرمجيات وكذلك للتحديث والترقية والتصحيح في حالة اكتشاف نقاط الضعف.

---

[٣] المنشور الخاص الصادر عن المعهد الوطني للمعايير والتكنولوجيا (NIST) ٨٠٠-٥٣، التنقيح ٥: https://doi.org/10.6028/NIST.SP.800-53r5.

[٤] عادة ما يُشار إلى نهج "الدفاع العميق" باسم "نهج القلعة" لأنه يعكس مستويات دفاعية كما في قلاع القرون الوسطى، التي كان يتعيَّن على مهاجميها مواجهة الخندق وجسر السحب والمتاريس والأبراج ...إلخ.

٤-٦ الأمن المادي

٤-٦-١ تشمل الأمثلة على الضوابط الأمنية المادية ذات الصلة بالأمن الإلكتروني في مجال الطيران، ضمن جملة أمور، تحديد سياسات إدارة ومراقبة النفاذ المادي، والتحقق من الخلفية الأمنية للموظفين من ذوي الحقوق الإدارية بشأن نُظُم/قواعد البيانات، أو ممن لديهم حق الوصول إلى البيانات الحسَّاسة و/أو الحرجة، والتوصيات المُتعلِّقة بفصل واجبات و/أو تناوب الموظفين الذين يتاح لهم إمكان الوصول إلى النُظُم الحيوية أو القدرة على تعديلها، الخ.

٤-٧ أمن تكنولوجيا المعلومات والاتصالات

٤-٧-١ من الأمثلة على ضوابط أمن تكنولوجيا المعلومات والاتصالات ذات الصلة بالأمن الإلكتروني في مجال الطيران، ضمن جملة أمور، سياسات مراقبة الدخول وتطبيق مبادئ أقل الامتيازات، وجدران الحماية للبرمجيات/الأجهزة، وأمن الشبكات، والتشفير، وسياسات كلمة المرور التنظيمية، وحماية النقاط النهائية، ورصد الشبكات والكشف عن الحالات الشاذة، وفصل الشبكات، وإدارة الأجهزة، وما إلى ذلك.

٤-٨ إدارة الوقائع واستمرارية المهام الحيوية

٤-٨-١ ينبغي للسلطة المختصَّة بالأمن الإلكتروني في مجال الطيران (AA/Cyber) أن تُحدِّد اللوائح والعمليات والمُتطلَّبات والأدوار في ما يتعلَّق بإدارة الوقائع الإلكترونية والتعافي من آثارها واستمرارية النُظُم الحرجة.

٤-٨-٢ وينبغي ترقية الخطط القائمة لإدارة الأزمات واستمرارية الأعمال لكي تشمل التصدِّي للوقائع الإلكترونية والتعافي من آثارها.

٤-٨-٣ وينبغي إجراء اختبار دوري لخطط الاستجابة لحالات الطوارئ واستمرارية الأعمال بهدف تحسين الخطط وكذلك قدرات المستجيبين. ويجب أن يشمل الاختبار جميع أصحاب المصلحة المعنيين وأن يضم مزيجاً من جلسات المحاكاة المكتبية بالإضافة إلى الاختبارات المباشرة.

٤-٩ ثقافة الأمن الإلكتروني

٤-٩-١ يجب تطبيق ثقافة الأمن الإلكتروني على نطاق جميع كيانات الطيران.

٤-٩-٢ وينبغي للقيادة التنظيمية أن تدعم ثقافة الأمن الإلكتروني، وأن تضع برنامجاً لذلك يضطلع به جميع الموظفين.

٤-٩-٣ ويجب أن يتضمن البرنامج توعية تكرارية بالأمن الإلكتروني (بما في ذلك مبادئ ممارسات النظافة الإلكترونية)، والتوعية بأحدث التهديدات وتنظيم دورات تدريبية وإجراء اختبارات (سواء كجزء من دورات التدريب أو المحاكاة الحية للهجمات) بهدف تقييم مستوى الوعي الإلكتروني/النظافة الإلكترونية.

٤-٩-٤ وينبغي أن تتضمن ثقافة الأمن الإلكتروني عناصر من ثقافات السلامة والأمن، على سبيل المثال، الإبلاغ الذاتي، والإبلاغ عن أنماط السلوك/الممارسات المشبوهة، وثقافة العدل، وما إلى ذلك.

— — — — — — — —

المرفق (أ)

نموذج لسياسة الأمن الإلكتروني

١- المقدمة

١-١ تكون سياسة الأمن الإلكتروني هذه إطاراً لمواصلة تطوير وتنفيذ الأمن الإلكتروني في مجال الطيران. وسيجري نشرها وتوزيعها على أصحاب المصلحة المعنيين، واستعراضها دورياً.

١-٢ ينبغي وضع المزيد من الإرشادات من أجل دعم تنفيذ سياسة الأمن الإلكتروني هذه.

٢- النطاق

٢-١ يعالج الأمن الإلكتروني في مجال الطيران القضايا المتصلة بالأمن الإلكتروني لنظام الطيران المدني وتعزيز قدرة هذه المنظومة على الصمود في وجه التهديدات والهجمات الإلكترونية، فضلاً عن دعم التعاون مع الكيانات والسلطات المعنية من خارج قطاع الطيران، بما في ذلك السلطة الوطنية للأمن الإلكتروني والأمن القومي وإنفاذ القانون والجيش، حسب الاقتضاء.

٢-٢ يجري تنسيق الأمن الإلكتروني في مجال الطيران على الصعيد الوطني مع سلامة الطيران وأمن الطيران وحماية البنية الأساسية الحيوية وشبكة الدفاع الإلكترونية والجيش.

٢-٣ يجري تنسيق الأمن الإلكتروني في مجال الطيران على الصعيد الدولي مع السلطات الأجنبية المناظرة المناسبة، المختصَّة بالأمن الإلكتروني في مجال الطيران.

٣- الأهداف

٣-١ تتمثل الأهداف العامة لسياسة الأمن الإلكتروني في مجال الطيران في ضمان أمن منظومة الطيران المدني وقدرتها على الصمود والتعزيز الذاتي في وجه التهديدات والهجمات الإلكترونية، وضمان تنسيق الأمن الإلكتروني في مجال الطيران مع السلطات والكيانات الوطنية المعنية.

٤- أساليب الإدارة والتنظيم

٤-١ بمقتضى [اللائحة/المرجع التشريعي للتعيين]، يكون [اسم الكيان] هو السلطة المختصة بالأمن الإلكتروني في مجال الطيران (AA/Cyber)، ولها ولاية عامة من أجل الأمن الإلكتروني في مجال الطيران وتعزيز قدرة الطيران المدني على الصمود في وجه التهديدات والهجمات الإلكترونية.

٤-٢ يجب على السلطة المختصة بالأمن الإلكتروني في مجال الطيران (AA/Cyber):

- الانخراط مع السلطة الوطنية المختصة بالأمن الإلكتروني من أجل تحديد أدوار ومسؤوليات الأمن الإلكتروني في مجال الطيران المدني التي تضطلع بها كل سلطة؛
- تنسيق عملية تطوير اللوائح التنظيمية المُتعلِّقة بالأمن الإلكتروني في مجال الطيران والمساهمة في تطويرها؛
- تحديد وتنسيق وتقديم الدعم من أجل السلطات المختصة بسلامة الطيران وأمن الطيران بغرض إدراج مُتطلَّبات الأمن الإلكتروني في مجال الطيران، بما في ذلك عناصر الإشراف ومراقبة الجودة، في البرنامج الوطني للسلامة (SSP) والبرنامج الوطني لأمن الطيران المدني (NCASP)؛
- تحديد ودعم ورصد تنفيذ برنامج تعزيز ثقافة الأمن الإلكتروني من قبل جميع أصحاب المصلحة في مجال الطيران المدني؛

- تحديد اللوائح التنظيمية والعمليات والمُتطلَّبات والأدوار من أجل إدارة أزمات الأمن الإلكتروني؛
- تنسيق القضايا الشاملة المتعلقة بالأمن الإلكتروني في مجال الطيران مع أصحاب المصلحة من خارج قطاع الطيران من المعنيين بالأمن الإلكتروني في مجال الطيران.

٥- إدارة المخاطر

٥-١ يجب أن يكون الأمن الإلكتروني مدفوعاً بقدرات استخبارية، وقائماً على التهديد، وأن تُطبق فيه منهجية إدارة المخاطر.

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

٥-٣ يجب أن تكون ملكية جميع البيانات والنُظُم مُحدَّدة في جميع الأوقات.

٦- أمن النُظُم الحرجة

٦-١ يجب تحديد الوظائف والنُظُم والبنية الأساسية الحيوية في عمليات إدارة المخاطر.

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

٦-٣ يُعتبر التكرار في النُظُم الحرجة عاملاً تمكينياً مساعداً لأمن النظام.

٧- أمن البيانات

٧-١ يجب حماية البيانات والمعلومات أثناء التخزين والإرسال، بما يتماشى مع مستوى حساسيتها.

٨- أمن سلسلة التوريد

٨-١ تكون الإدارة الشاملة على طول سلسلة توريد البرمجيات/المعدات جزءًا من إدارة الأمن الإلكتروني في مجال الطيران.

٨-٢ يجب أن تتوافق البرمجيات والأجهزة المستخدمة في وظائف الطيران الحرجة مع مُتطلَّبات الأمن الإلكتروني طوال دورة حياة نُظُم الطيران.

٩- الأمن المادي

٩-١ يكون الأمن المادي (بما في ذلك أمن الموظفين) جزءًا من إدارة الأمن الإلكتروني في مجال الطيران.

٩-٢ الغرض من الأمن المادي هو حماية الأشخاص والبنية الأساسية والمرافق والمعدات والمواد والوثائق من أي تدخل غير مشروع، وحماية نُظُم الطيران الحيوية من الوصول المادي غير المصرح به.

٩-٣ يُسهم الأمن المادي في إدارة المخاطر من خلال دعم تحديد الكيانات المُهدِّدة و/أو احتمال شن هجمات على البنية الأساسية الحيوية للطيران المدني.

١٠- أمن تكنولوجيا المعلومات والاتصالات

١٠-١ يكون أمن تكنولوجيا المعلومات والاتصالات جزءًا من إدارة الأمن الإلكتروني في مجال الطيران.

١٠-٢ يحدد أمن تكنولوجيا المعلومات والاتصالات تدابير أمن منطقية وينفِّذُها، فضلاً عن المساهمة في عمليات إدارة الوقائع الإلكترونية، والتعافي من آثارها، وفي استمرارية التشغيل.

١٠-٣ يُسهم أمن تكنولوجيا المعلومات والاتصالات في إدارة المخاطر من خلال تحديد نقاط الضعف، وناقلات الهجمات، ورصد تطوُّر مشهد تهديد الأمن الإلكتروني في مجال الطيران.

١١- إدارة الوقائع واستمرارية المهام الحيوية

١١-١ المحرِّك الأساسي لعمليات إدارة الوقائع هو سلامة العمليات واستمرارية المهام الحيوية.

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

١٢- ثقافة الأمن الإلكتروني

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

١٢-٢ يجب تنسيق ثقافة الأمن الإلكتروني بشكل كامل مع ثقافات السلامة والأمن القائمة.

١٢-٣ يجب دعم ثقافة الأمن الإلكتروني بممارسات قوية لتبادل المعلومات داخلياً، وبالقدر الممكن، خارجياً.

— انتهى —