دليل استبيان الرقم القياسي العالمي للأمن السيبراني (GCI) للعام 2018

هذه الوثيقة للعلم فقط. يقيس الرقم القياسي العالمي للأمن السيبراني التزام البلدان في مجال الأمن السيبراني وفقاً للدعائم الخمس للبرنامج العالمي للأمن السيبراني: التدابير القانونية والتدابير التقنية والتدابير التنظيمية وبناء القدرات والتعاون.

وقد تم في هذا الاستبيان دمج الأسئلة التي صيغت من أجل تحديد درجات الرقم القياسي العالمي للأمن السيبراني للعام 2018/2017 مع الأسئلة المطلوبة في المسألة 3 للجنة الدراسات 2 لقطاع تنمية الاتصالات. ويتألف الاستبيان من خمسة أقسام منفصلة، حيث تكون الإجابة على أسئلة كل الأقسام بنعم/لا وتكون مصحوبة بمربعات لوضع علامة عليها قبل كل عنصر. وينبغي استكمال الاستبيان على الخط. وسيزود كل مستجيب (عن طريق رسالة إلكترونية رسمية من الاتحاد) بموقع إلكتروني (URL) فريد للحفظ الآمن لبياناته. ويمكّن الاستبيان على الخط المستجيبين من وضع الوثائق ذات الصلة (والمواقع الإلكترونية) لكل سؤال كمعلومات داعمة.

المعلومات المقدمة من المستجيبين لهذا الاستبيان يفترض ألا تكون سرية الطابع.

1 التدابير القانونية

1.1 هل هناك قانون متعلق بالجريمة السيبرانية؟

الشرح: *تشير تشريعات الجريمة السيبرانية إلى أي قانون يحمي سرية وسلامة وتوافر أنظمة الحاسوب والشبكات والبيانات الحاسوبية؛ والجرائم المتعلقة بالحاسوب؛ والجرائم المتعلقة بالمحتوى؛ والجرائم المتعلقة بانتهاكات حقوق النشر والحقوق ذات الصلة. وتشمل أيضاً القوانين الإجرائية والمساعدة المتبادلة.*

- ☐ *نعم*
- ☐ *لا*
- ☐ *جزئي (لا تكون **إلا** مسودات في مرحلة متقدمة وجاهزة للاعتماد أو التحقق منها)*

1.1.1 هل هناك قانون موضوعي بشأن...

الشرح: *يشير مصطلح القانون الموضوعي إلى القانون الذي يؤسس الحقوق ويحددها وينظمها.* **(يرجى التحديد عن طريق وضع علامة في مربع مادة (مواد) ما تنطبق على بلدك وضع علامة على الصفحات ورقم المادة (المواد) التي توجد فيها المواد التالية في وثائقك)**

- ☐ النفاذ غير المخوَّل إلى أجهزة الحاسوب والأنظمة والبيانات؟
- ☐ التداخل/الاعتراض/التعديل/التدمير غير المخوَّل على أجهزة الحاسوب والأنظمة والبيانات؟
- ☐ حماية البيانات/الخصوصية؟

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

شرح قانون جزئي أو مادة جزئية من خلال تقديم مسودات المواد المذكورة أعلاه فقط.

2.1.1 هل هناك قانون إجرائي للجريمة السيبرانية متعلق بما يلي:

الشرح: *القانون الإجرائي* يشير إلى القواعد والشكليات التي يتعين اتباعها في إجراء قانوني من أجل ضمان تطبيق القانون بصورة عادلة ومتسقة في جميع القضايا التي تعرض على المحكمة. **(يرجى التحديد عن طريق وضع علامة في مربع مادة ما تنطبق على بلدك وضع علامة على الصفحات وعدد المواد التي توجد فيها المواد التالية في وثائقك).**

- ☐ مواد عن الحفظ السريع للبيانات الحاسوبية المخزنة
- ☐ مواد بخصوص أوامر الإفصاح
- ☐ مواد بخصوص البحث في البيانات الحاسوبية المخزنة والتحفظ عليها
- ☐ مواد تتعلق بجمع البيانات الحاسوبية في الوقت الفعلي
- ☐ مواد تتعلق بتسليم المجرمين السيبرانيين
- ☐ مواد تتعلق بالمساعدة المتبادلة
- ☐ مواد تتعلق بالسرية أو تقييد الاستعمال

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

شرح قانون جزئي أو مادة جزئية من خلال تقديم مسودات المواد المذكورة أعلاه فقط.

2.1 هل هناك أي لوائح للأمن السيبراني متعلقة بما يلي:

الشرح: *اللوائح: قواعد يستند إليها أو يقصد بها تنفيذ جزء محدد من التشريعات. تقوم بإنفاذ اللوائح عادةً* ***الهيئات التنظيمية*** *التي يوكل إليها تنفيذ أهداف أو أحكام أي تشريع. ومن هنا، فإن تنظيم الأمن السيبراني ينطوي على وضع مبادئ تلتزم بها الأطراف المعنية، تنشأ وتشكل جزءاً من عملية تنفيذ القوانين التي تتناول* **(يرجى التحديد عن طريق وضع علامة في مربع مادة ما تنطبق على بلدك وضع علامة على الصفحات وعدد المواد التي توجد فيها المواد التالية في وثائقك).** ويرجى الإحاطة علماً بأن هذا القسم مخصص للوائح فقط وليس للقوانين/التشريعات المشار غليها في السؤال 1.1.1.

- ☐ *نعم*
- ☐ *لا*
- ☐ *جزئي*

- ☐ حماية البيانات؟
- ☐ انتهاكات الخصوصية؟
- ☐ متطلبات تدقيق الأمن السيبراني وشهادات/تقييس الأمن السيبراني؟
- ☐ حماية الخصوصية؟
- ☐ التوقيعات الرقمية والمعاملات الإلكترونية؟
- ☐ مسؤولية موردي خدمات الإنترنت؟
- ☐ النظام وحماية الشبكة؟

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

شرح قانون جزئي أو مادة جزئية من خلال تقديم مسودات المواد المذكورة أعلاه فقط.

3.1 هل توجد تشريعات أو لوائح متعلقة باحتواء أو كبح الرسائل الاقتحامية؟

الشرح: *يشير إلى التشريعات/اللوائح المتعلقة بالحماية من الرسائل الإلكترونية غير المطلوبة الناتجة عن استخدام الإنترنت. (يرجى الإشارة إلى اللوائح أو التشريعات (القانون) أو الاثنين).*

- ☐ نعم
- ☐ لا
- ☐ جزئي

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

شرح قانون جزئي أو مادة جزئية من خلال تقديم مسودات المواد المذكورة أعلاه فقط.

4.1 يرجى تقديم بعض من أفضل الممارسات/الإنجازات/حالات التقدم التي اشترك/يشترك فيها بلدك فيما يتعلق بالمجالات القانونية كجزء من أنشطة الأمن السيبراني. (ملاحظة: أفضل الممارسات لا تنطبق إلا على البلدان التي لديها قوانين أو لوائح متعلقة بالأمن السيبراني)

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

يرجى إدراج قائمة أفضل الممارسات هنا إذا لم يكن هناك رابط أو وثيقة أعلاه

2 التدابير التقنية

1.2 هل لديكم فريق للاستجابة للحوادث الحاسوبية (CIRT) أو فريق للاستجابة للحوادث الأمنية الحاسوبية (CSIRT) أو فريق للاستجابة للطوارئ الحاسوبية (CERT)؟

الشرح: *يشير المختصر CIRT إلى فريق الاستجابة للحوادث الحاسوبية. ويشير المختصر CSIRT إلى فريق الاستجابة للحوادث الأمنية الحاسوبية. ويشير المختصر CERT إلى فريق الاستجابة للطوارئ الحاسوبية. وتستخدم هذه المصطلحات بالتبادل للإشارة إلى أي كيان تتلقى تقارير المخالفات الأمنية ويقوم بإجراء التحليلات لهذه التقارير والرد على الجهة المرسلة.*

- ☐ نعم
- ☐ لا

1.1.2 يرجى بيان أي فريق من أفرقة CERT أو CIRT أو CSIRT ينطبق في حالة بلدك.

الشرح: *ويشير مصطلح فريق CERT/CIRT/CSIRT وطني إلى أي كيان أوكلت إليه مسؤولية مراقبة وإدارة والتعامل مع حوادث الأمن السيبراني مع الجهات المحلية التابعة له بما في ذلك الهيئات الأكاديمية وهيئات إنفاذ القانون والمجتمع المدني والقطاع الخاص (في مجموعات اقتصادية أو مجموعات حساسة أو البنى التحتية الحرجة للمعلومات (الطاقة والصحة والنقل والشؤون المالية وغيرها)) والحكومة. ويتعامل هذا الكيان أيضاً مع أفرقة الاستجابة للحوادث الحاسوبية الوطنية الخاصة بالبلدان الأخرى. فضلاً عن الأطراف الفاعلة الإقليمية والدولية بشأن التنسيق ذي الصلة والفعال في حالة وقوع هجمات حاسوبية.*

- ☐ فريق CERT أو CIRT أو CSIRT وطني
- ☐ فريق CERT أو CIRT أو CSIRT حكومي
- ☐ فريق CERT أو CIRT أو CSIRT قطاعي

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

2.2 هل تجري هذه الأفرقة تمارين مستمرة للأمن السيبراني؟

الشرح: *حادث مرتب تقوم خلاله منظمة ما بمحاكاة خلل سيبراني من أجل تطوير أو اختبار إمكانات المنع أو الاكتشاف أو التخفيف من الآثار أو الاستجابة أو الاستعادة فيما يتعلق بحالات الخلل هذه. وهل يجري هذا التمرين بصورة دورية أو متكررة؟*

- ☐ نعم
- ☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

3.2 هل الأفرقة CIRT أو CSIRT أو CERT المختارة أعلاه منتسبة/منضمة إلى

- ☐ منتدى أفرقة الأمن والاستجابة للحوادث (FIRST)
- ☐ أفرقة CERTS الإقليمية *(APCERT، ICCERT، AFRICERT، TFCCERT)*
- ☐ أي من رابطات CERT الأخرى

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

4.2 هل هناك أي إطار لتنفيذ معايير الأمن السيبراني؟

الشرح: *وجود إطار (أطر) معتمدة من الحكومة (أو تحظى بتأييدها) من أجل تنفيذ معايير الأمن السيبراني المعترف بها دولياً داخل القطاع العام (الوكالات الحكومية) وداخل البنى التحتية الحرجة (حتى ولو كان القطاع الخاص يقوم بتشغيلها). وتشمل هذه المعايير، على سبيل المثال لا الحصر، تلك التي تضعها الوكالات التالية: المنظمة الدولية للتوحيد القياسي (ISO)، والاتحاد الدولي للاتصالات (ITU)، وفريق مهام هندسة الإنترنت (IETF)، ومعهد مهندسي الكهرباء والإلكترونيات (IEEE)، وتحالف حلول صناعة الاتصالات (ATIS)، ومنظمة تقدم معايير المعلومات المهيكلة (OASIS)، ومشروع شراكة الجيل الثالث (3GPP)، والمشروع 2 لشراكة الجيل الثالث (3GPP2)، ومجلس تصميم الإنترنت (IAB)، وجمعية الإنترنت (ISOC)، ومجموعة السلامة على الإنترنت (ISG)، وفريق التداخل بين الرموز (ISI)، والمعهد الأوروبي لمعايير الاتصالات (ETSI)، وقوات الأمن الداخلي (ISF)، وRFC، والمعايير الدولية لمراجعة الحسابات (ISA)، واللجنة الكهرتقنية الدولية (IEC)، والمجلس الوطني للبحوث البيئية (NERC)، والمعهد الوطني للمعايير والتكنولوجيا (NIST)، ومعايير معالجة المعلومات الفيدرالية (FIPS)، ومعلومات التحكم بالبروتوكول (PCI)، وخدمة أمن الدفاع (DSS)، وغيرها.*

- ☐ في القطاع العام
- ☐ في القطاع الخاص

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

5.2 هل لديكم هيئة تقييس في البلد

- ☐ توفر معاييرها الذاتية بشأن الأمن السيبراني
- ☐ أو تعتمد المعايير الدولية

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

6.2 هل هناك أي آليات وإمكانات تقنية مستخدمة لمكافحة الرسائل الاقتحامية؟

الشرح: *هل هناك أدوات وتدابير تقنية معنية متعلقة بتوفير الأمن السيبراني، مثل برمجيات مكافحة الفيروسات والرسائل الاقتحامية؟*

- ☐ نعم
- ☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

7.2 هل يستخدم بلدك أو منظمتك السحاب لأغراض الأمن السيبراني في القطاع العام؟

الشرح: *برمجية لضمان النسخ الرديف للبيانات في حالة التداخل غير المطلوب عبر الإنترنت أو الحاسوب بخلاف استخدام برمجيات مكافحة الفيروسات ومجموعات برمجيات أمن الإنترنت والبرمجيات الضارة والتجفير لتحسين أنظمة الأمن السيبراني الحكومية. ويسمح النظام الحاسوبي للفرد باستخدام وثائقه/بياناته أو أي مواد محفوظة والنفاذ إليها من أي مكان وفي أي وقت بدون الأضرار التي يتسبب فيها التداخل الحاسوبي عند طرف ما. (مرة أخرى، يتمثل الهدف من هذا السؤال في فهم الاستعمال المحتمل للسحاب لتحسين وضع الأمن السيبراني على المستوى الوطني بدون تحديد برمجية معينة في السحاب)*

☐ نعم

☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

8.2 يرجى تقديم بعض من أفضل الممارسات/الإنجازات/حالات التقدم التي اشترك/يشترك فيها بلدك فيما يتعلق بالمجالات التقنية كجزء من أنشطة الأمن السيبراني. (ملاحظة: أفضل الممارسات لا تنطبق إلا على البلدان التي لديها أفرقة **CIRT** أو **CSIRT** أو **CERT**)؟

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

3 التدابير التنظيمية

1.3 هل توجد استراتيجية (سياسة) وطنية للأمن السيبراني؟

الشرح: *تتمثل السياسات المعنية بالاستراتيجيات الوطنية للأمن السيبراني أو الخطط الوطنية لحماية البنى التحتية للمعلومات بتلك التي تحددها الدولة القومية وتقرها بشكل رسمي، وقد تنطوي على الالتزامات التالية: تحديد مسؤولية واضحة بشأن الأمن السيبراني على جميع مستويات الحكم (المحلي أو الإقليمي أو الاتحادي أو الوطني)، مع أدوار ومسؤوليات محددة بوضوح؛ وتقديم تعهد واضح بالأمن السيبراني يكون عاماً وشفافاً؛ وتشجيع إشراك القطاع الخاص والشراكة معه في المبادرات التي ترأسها الحكومة من أجل تعزيز الأمن السيبراني، ووضع خارطة طريق للإدارة تحدد أصحاب المصلحة الأساسيين. (إذا كانت الاستراتيجية لا تزال قيد الإعداد، يرجى وضع علامة على المربع "جزئي" والانتقال مباشرة إلى السؤال 8.3 وإذا لم تكن هناك أي استراتيجية، يرجى الانتقال مباشرة إلى السؤال 8.3 أيضاً)*

- ☐ نعم
- ☐ لا
- ☐ جزئي (لا تكون **إلا** مسودات في مرحلة متقدمة وجاهزة للاعتماد أو التحقق منها)

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

شرح مسودة جزئية من خلال تقديم مسودات الاستراتيجية الوطنية.

2.3 هل الاستراتيجية الوطنية

الشرح: *قد تكون الاستراتيجية الوطنية للأمن السيبراني موجودة في وثيقة منفصلة عن الاستراتيجية الوطنية للمعلومات أو التكنولوجيا أو الأمن* (إذا كنت قد قمت بتحميل الاستراتيجية في السؤال أعلاه، لا توجد حاجة إلى تحميل الوثيقة مرتين، ويرجى مجرد الإشارة إلى رقم الصفحة التي تتضمن إثباتات ذات الصلة بالأسئلة الواردة أدناه حتى السؤال 5.3)

- ☐ قائمة بذاتها؟
- ☐ أو مدرجة في استراتيجية وطنية أخرى أوسع نطاقاً؟

يرجى تقديم رقم الصفحة

3.3 هل تتناول الاستراتيجية

الشرح: *تحدد الاستراتيجية أدوار ومسؤوليات الأمن السيبراني بالنسبة للأطراف الفاعلة في القطاع الخاص أو في القطاع العام.*

- ☐ القطاع الخاص؟
- ☐ القطاع العام؟

يرجى تقديم رقم الصفحة

4.3 هل يوجد قسم عن:

الشرح: *تتضمن الاستراتيجية خططاً لحماية البنى التحتية الحرجة للمعلومات.*

الشرح: *تضمن خطة التعافي الوطنية تعافي البلاد من آثار أي كارثة (طبيعية أو اصطناعية) في الوقت المناسب وبكفاءة، بما في ذلك من خلال حفظ واستعادة هياكلها ووظائفها الأساسية.*

- ☐ حماية البنى التحتية الحرجة للمعلومات؟
- ☐ خطة وطنية بشأن التعافي؟

يرجى تقديم رقم الصفحة

5.3 هل هناك خطة عمل حكومية واضحة للتنفيذ بشأن حوكمة الأمن السيبراني؟

الشرح: *تشتمل الاستراتيجية على خريطة طريق/استراتيجية تتضمن مراحل رئيسية لإنجاز وإكمال الاستراتيجية.*

- ☐ نعم
- ☐ لا

يرجى تقديم رقم الصفحة

6.3 هل الاستراتيجية

- ☐ تُراجع بشكل مستمر؟
- ☐ مفتوحة أمام المشاورات العامة؟

الشرح: *تُحدث الاستراتيجية طبقاً للتطورات الوطنية والتكنولوجية والاجتماعية والاقتصادية والسياسية التي يمكن أن تؤثر عليها.*

الشرح: *تكون الاستراتيجية مفتوحة للتشاور بالنسبة لجميع أصحاب المصلحة المعنيين، بما في ذلك مشغلو البنى التحتية وموردو خدمات الإنترنت والهيئات الأكاديمية وما إلى ذلك.*

يرجى تقديم رقم الصفحة أو
تقديم رابط يشير إلى المشاورة المفتوحة

7.3 هل توجد جهة/وكالة وطنية مسؤولة عن:

- ☐ الأمن السيبراني وحماية البنى التحتية للمعلومات الحرجة
- ☐ نقطة اتصال/وكالة/مبادرات بشأن بالمسائل المتعلقة بمكافحة الرسائل الاقتحامية؟

الشرح: *الوكالة المسؤولة عن تنفيذ الاستراتيجية/السياسات الوطنية للأمن السيبراني يمكن أن تضم لجاناً دائمة أو أفرقة عمل رسمية أو مجالس استشارية أو مراكز متعددة الاختصاصات. وقد يتولى كيان كهذا المسؤولية المباشرة للفريق CIRT الوطني. وقد تكون الوكالة المسؤولة داخل الحكومة أو قد تكون لها سلطة ضم وكالات وهيئات وطنية أخرى لتنفيذ السياسات واعتماد المعايير.*

- ☐ نعم
- ☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)
يرجى تقديم الوثائق

8.3 هل توجد أي مقاييس لقياس تطور الأمن السيبراني على المستوى الوطني؟

الشرح: *وجود أي ممارسات تقييم وطنية أو قطاعية معترف بها أو يفضل استعمالها في قياس تطور الأمن السيبراني واستراتيجيات تقييم المخاطر ومراجعات الأمن السيبراني وغيرها من الأدوات والأنشطة الخاصة بقياس أو تقييم الأداء الناتج من أجل إجراء تحسينات في المستقبل. على سبيل المثال، طبقاً للمعيار ISO/IEC 27004 المعني بالقياسات المتعلقة بإدارة أمن المعلومات.*

- ☐ نعم
- ☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

9.3 هل تجرى تقييمات المخاطر دورياً؟

الشرح: *عملية نظامية تشمل تحديد المخاطر وتحليلها وتقييمها.*

- ☐ نعم
- ☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

10.3 هل توجد مقاييس مرجعية بشأن الأمن السيبراني لتقييم المخاطر؟

- ☐ نعم
- ☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

11.3 هل تجرى مراجعات عامة للأمن السيبراني؟

الشرح: *المراجعة الخاصة بالأمن هي تقييم نظامي لأمن أحد أنظمة المعلومات عن طريق قياس إلى أي مدى يلتزم بمجموعة من المعايير المحددة. والمراجعة الكاملة تتولى عادةً تقييم أمن التشكيلة المادية للنظام والبيئة والبرمجيات وعمليات تداول المعلومات وممارسات المستعملين.*

- ☐ نعم
- ☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

12.3 يرجى تقديم بعض من أفضل الممارسات/الإنجازات/حالات التقدم التي اشترك/يشترك فيها بلدك فيما يتعلق بالتدابير التنظيمية كجزء من أنشطة الأمن السيبراني.

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

4 أنشطة بناء القدرات

1.4 هل يتم إطلاق وتنفيذ حملات للوعي العام بالأمن السيبراني؟

الشرح: *يشمل الوعي العام الجهود التي تبذل في سبيل تشجيع حملات الإعلان الواسعة الانتشار لكي تصل إلى أكبر عدد ممكن من الأشخاص والاستفادة من المنظمات غير الحكومية والمؤسسات والمنظمات وموردي خدمات الإنترنت والمكتبات ومنظمات التجارة المحلية والمراكز المجتمعية متاجر الحواسيب وكليات المجتمعات المحلية وبرامج تعليم الكبار والمدارس ومنظمات الأهل–المعلمين من أجل توصيل الرسالة إلى الجميع بشأن السلوك الآمن من الناحية السيبرانية على الشبكة. ويتضمن ذلك إجراءات من قبيل إنشاء بوابات ومواقع شبكية لإذكاء الوعي، ونشر مواد الدعم وإرساء اعتناق مفهوم الأمن السيبراني.*

- ☐ نعم
- ☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

2.4 هل تستهدف حملات التوعية العامة:

- ☐ المنظمات؟
- ☐ المجتمع المدني؟
- ☐ البالغين؟
- ☐ الشباب والأطفال؟
- ☐ الهيئات الأخرى ذات الصلة؟

يرجى تقديم روابط مرقمة/محددات موارد موحدة (URL) مرقمة على التوالي لكل مربع تختاره من المربعات الواردة أعلاه

يرجى تقديم وثائق مرقمة لكل مربع تختاره من المربعات الواردة أعلاه على التوالي

3.4 هل هناك أي إطار لمنح الشهادات للمهنيين العاملين في مجال الأمن السيبراني واعتمادهم؟

الشرح: *وجود إطار (أو أطر) معتمدة من الحكومة (أو تحظى بموافقتها) من أجل منح الشهادات للمهنيين واعتمادهم من خلال معايير للأمن السيبراني معترف بها دولياً. وتتضمن هذه الشهادات والاعتمادات والمعايير، على سبيل المثال لا الحصر، ما يلي: معرفة أمن الحوسبة السحابية (التحالف المعني بأمن الحوسبة السحابية)، وCISSP، وSSCP، وCBK CSSLP، والتحليل الجنائي في مجال الأمن السيبراني (ISC²) وGIAC وGIAC GSSP (SANS) وCISM وCISA وCRISC (ISACA) والرابطة الصناعية لتكنولوجيا الحوسبة (CompTIA) وC|CISCO وCEH وECSA وCHFI (مجلس المجموعة الأوروبية) وOSSTMM (ISECOM) وPCIP/CCISP (معهد البنى التحتية الأساسية) ومنح الشهادات (بدون اقتراحات) وQ/ISP ومنح شهادة هندسة أمن البرمجيات (جامعة الأمن) وCPP وPSP وPCI (ASIS) وLPQ وLPC (معهد منع الخسائر)، ورابطة مفتشي الاحتيال المعتمدين (CFE)، ومعالجو حوادث الأمن الحاسوبي المعتمدون من الفريق الوطني لمواجهة الطوارئ الحاسوبية (SEI)، ومعهد التعليم المالي الاستهلاكي (CITRMS)، ومعهد الأمن السيبراني (CSFA) وCIPP (IAPP) وABCP وCBCP وMBCP (DRI) وBCCP وBCCS وBCCE وDRCS وDRCE (BCM) وCIA وCCSA (معهد المراجعين الداخليين)، والرابطة الدولية لمديري المخاطر المتخصصين، ومعهد إدارة المشاريع (PMP)، إلخ.*

- ☐ في القطاع الخاص
- ☐ في القطاع العام

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

4.4 هل تقوم حكومتكم/منظمتكم بوضع أو دعم أي دورات تدريبة مهنية في مجال الأمن السيبراني...

الشرح: *وجود برامج تدريب تعليمية ومهنية وطنية أو قطاعية، تنهض بمناهج الأمن السيبراني لقوة العمل (تقنية واجتماعية وعلوم وما إلى ذلك) وتنهض بمنح الشهادات للمهنيين في كل من القطاعين العام أو الخاص.*

- ☐ لمسؤولي إنفاذ القانون (ضباط الشرطة ووكلاء إنفاذ القانون)؟
- ☐ للعاملين في الجهاز القضائي وغيرهم من المسؤولين القانونيين (القضاة ووكلاء النيابة والمحامون في المحاكم العليا والمحامون ومساعدو المحامين، وما إلى ذلك)؟
- ☐ للمنظمات؟
- ☐ للقطاع العام؟
- ☐ للمجتمع المدني؟
- ☐ لجهات أخرى؟

يرجى تقديم روابط مرقمة/محددات موارد موحدة (URL) مرقمة على التوالي لكل مربع تختاره من المربعات الواردة أعلاه

يرجى تقديم وثائق مرقمة لكل مربع تختاره من المربعات الواردة أعلاه على التوالي

5.4 هل تقوم حكومتكم/منظمتكم بوضع أو دعم أي برامج تعليمية أو مناهج أكاديمية في مجال الأمن السيبراني...

الشرح: *وجود وتشجيع مناهج وبرامج تعليم وطنية لتدريب جيل الشباب على المهارات والمهن المتعلقة بالأمن السيبراني في المدارس والكليات والجامعات ومؤسسات التعلم الأخرى: وتشمل المهارات المتعلقة بالأمن السيبراني، على سبيل الذكر وليس الحصر، استنباط كلمات مرور قوية وعدم الكشف عن المعلومات الشخصية على الخط. وتشمل المهن المتعلقة بالأمن السيبراني، على سبيل الذكر وليس الحصر، محللي الشفرات وخبراء الأدلة الجنائية الرقمية والمستجيبين لحالات الحوادث والمعماريين الآمنين ومختبري الاختراق.*

- ☐ في المدارس الابتدائية؟
- ☐ في المدارس الثانوية؟
- ☐ في مؤسسات التعليم العالي؟
- ☐ في مؤسسات أخرى؟

يرجى تقديم روابط مرقمة/محددات موارد موحدة (URL) مرقمة على التوالي لكل مربع تختاره من المربعات الواردة أعلاه

يرجى تقديم وثائق مرقمة لكل مربع تختاره من المربعات الواردة أعلاه على التوالي

6.4 هل يوجد استثمار في برامج البحث والتطوير الخاصة بالأمن السيبراني؟

الشرح: *تشمل برامج البحث الخاصة بالأمن السيبراني، على سبيل الذكر وليس الحصر، تحليل البرمجيات الضارة وعلم التشفير والبحث في مواطن ضعف الأنظمة ونماذج ومفاهيم الأمن. وتشير برامج التطوير الخاصة بالأمن السيبراني إلى تطوير حلول خاصة بالعتاد أو البرمجيات تشمل، على سبيل الذكر وليس الحصر، جدران الحماية وأنظمة منع الاقتحام ومضادات البرمجيات الروبوتية لوحدات النمطية لأمن العتاد. ومن شأن وجود هيئة وطنية شاملة أن يزيد التنسيق بين مختلف المؤسسات وتقاسم الموارد.*

- ☐ في القطاع العام
- ☐ في القطاع الخاص
- ☐ في مؤسسات التعليم العالي (الهيئات الأكاديمية)
- ☐ هيئة مؤسسية معترف بها وطنياً للإشراف على أنشطة البحث والتطوير في مجال الأمن السيبراني
- ☐ هيئة مؤسسية معترف بها للإشراف على أنشطة بناء القدرات في مجال الأمن السيبراني
- ☐ أخرى

يرجى تقديم روابط مرقمة/محددات موارد موحدة (URL) مرقمة على التوالي لكل مربع تختاره من المربعات الواردة أعلاه

يرجى تقديم وثائق مرقمة لكل مربع تختاره من المربعات الواردة أعلاه على التوالي

7.4 هل هناك أي آليات لتقديم حوافز حكومية من أجل تشجيع بناء القدرات في مجال الأمن السيبراني؟

الشرح: *أي جهود تحفيزية تبذلها الحكومة لتشجيع بناء القدرات في مجال الأمن السيبراني، سواء من خلال الإعفاءات الضريبية وتقديم المنح والقروض وتدبير المرافق وغيرها من الحوافز الاقتصادية والمالية، بما في ذلك تخصيص هيئة مؤسسية معترف بها وطنياً للإشراف على أنشطة بناء القدرات في مجال الأمن السيبراني. وتزيد الحوافز من الطلب على الخدمات والمنتجات المتعلقة بالأمن السيبراني، مما يحسن من القدرات الدفاعية في مواجهة التهديدات السيبرانية.*

- ☐ نعم
- ☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

8.4 هل توجد صناعة داخلية للأمن السيبراني؟

الشرح: *من شأن وجود بيئة اقتصادية وسياسية واجتماعية مؤاتية تدعم تطوير الأمن السيبراني أن يحفز وجود ونمو قطاع خاص حول الأمن السيبراني. ووجود حملات للوعي العام وتنمية لقوة العمل وبناء للقدرات وحوافز حكومية من شأنه أن يدفع بظهور سوق لمنتجات وخدمات الأمن السيبراني. ووجود صناعة داخلية للأمن السيبراني يعد شاهداً على هذه البيئة المؤاتية وسيدفع بنمو المشاريع المبتدئة في مجال الأمن السيبراني وأسواق التأمين السيبراني المرتبطة بها.*

- ☐ نعم
- ☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

9.4 هل توجد سوق للتأمين السيبراني؟

الشرح: *التأمين السيبراني هو منتج تأميني يستعمل لحماية الشركات وفرادى المستعملين من المخاطر القائمة على الإنترنت ومن منظور أوسع من المخاطر المتعلقة بالبنية التحتية والأنشطة الخاصة بتكنولوجيا المعلومات.*

- ☐ نعم
- ☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

10.4 هل يقدم أي دعم للمشاريع المبتدئة في مجال الأمن السيبراني وللتطوير؟

الشرح: *وجود آليات لدعم تطوير مشاريع مبتدئة في مجال الأمن السيبراني (حوافز ضريبية ومجمعات التكنولوجيا ومناطق للتجارة الحرة وما إلى ذلك) وللشركات الصغيرة والمتوسطة (SME).*

- ☐ نعم
- ☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

11.4 يرجى تقديم بعض من أفضل الممارسات/الإنجازات/حالات التقدم التي اشترك/يشترك فيها بلدك فيما يتعلق بتدابير بناء القدرات كجزء من أنشطة الأمن السيبراني

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

يرجى إدراج قائمة أفضل الممارسات هنا إذا لم يكن هناك رابط أو وثيقة أعلاه

5 التدابير التعاونية

1.5 هل هناك أي اتفاقات ثنائية بشأن التعاون في مجال الأمن السيبراني مع:

الشرح: *تشير الاتفاقات الثنائية (اتفاقات بين طرفين) إلى أي شراكات وطنية أو قطاعية معترف بها رسمياً لتبادل معلومات الأمن السيبراني أو أصوله عبر الحدود بين الحكومة وحكومة أجنبية أخرى أو كيان إقليمي أو منظمة دولية (أي التعاون أو تبادل المعلومات والخبرات والتكنولوجيات والموارد الأخرى).*

- ☐ الدول الوطنية أو الدول الأعضاء
- ☐ المنظمات الدولية
- ☐ جهات أخرى

2.5 هل الاتفاق/الاتفاقات

- ☐ ملزم قانوناً
- ☐ لتبادل المعلومات
- ☐ لتبادل الأصول
- ☐ غير ملزم قانوناً (غير رسمي)
- ☐ في انتظار التصديق

3.5 هل توجد أي اتفاقات متعددة الأطراف بشأن التعاون في مجال الأمن السيبراني؟

الشرح: *تشير الاتفاقات متعددة الأطراف (اتفاقات بين طرف وأطراف متعددة) إلى أي برامج وطنية أو قطاعية معترف بها رسمياً من أجل تبادل معلومات أو أصول الأمن السيبراني عبر الحدود بين الحكومة وحكومات أجنبية أو منظمات دولية متعددة (أي التعاون أو تبادل المعلومات والخبرات للتكنولوجيات والموارد الأخرى). وقد تشمل كذلك التصديق على اتفاقات دولية بخصوص الأمن السيبراني، مثل اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية واتفاقية بودابيست بشأن الجريمة السيبرانية وغيرها.*

- ☐ نعم
- ☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

4.5 هل الاتفاق

- ☐ ملزم قانوناً
- ☐ لتبادل المعلومات
- ☐ لتبادل الأصول
- ☐ غير ملزم قانوناً (غير رسمي)
- ☐ في انتظار التصديق

5.5 هل تشارك حكومتكم/منظمتكم في منتديات/رابطات دولية معنية بالأمن السيبراني؟

☐ نعم

☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

6.5 هل توجد أي شراكات بين القطاعين العام والخاص...

الشرح: *يشير مصطلح الشراكات بين القطاعين العام والخاص (PPP) إلى مشاريع مشتركة بين القطاعين العام والخاص. ويمكن قياس مؤشر الأداء هذا من خلال عدد الشراكات الوطنية أو القطاعية المعترف بها رسمياً بين القطاعين العام والخاص لتبادل معلومات الأمن السيبراني (معلومات التهديدات) وأصوله (الأشخاص والعمليات والأدوات) بين القطاعين العام والخاص (أي الشراكات الرسمية للتعاون أو تبادل المعلومات و/أو الخبرات و/أو التكنولوجيا و/أو الموارد)، وطنياً أو دولياً.*

☐ مع شركات محلية؟

☐ مع شركات أجنبية؟

7.5 هل توجد أي شراكات على النحو التالي:

الشرح: *يشير مؤشر الأداء هذا إلى أي شراكات رسمية بين الوكالات الحكومية المختلفة داخل دولة وطنية (لا يشير إلى الشراكات الدولية). ويمكن أن تسير إلى الشراكات بشأن تبادل المعلومات أو الأصول بين الوزارات والدوائر الحكومية والبرامج ومؤسسات القطاع العام الأخرى.*

☐ شراكات بين الوكالات؟

☐ شركات داخل الوكالات؟

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

8.5 يرجى تقديم بعض من أفضل الممارسات/الإنجازات/حالات التقدم التي اشترك/يشترك فيها بلدك فيما يتعلق بالتدابير التعاونية كجزء من أنشطة الأمن السيبراني

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

6 استقصاء تكميلي: حماية الأطفال على الخط

1.6 هل هناك أي تدابير لحماية الأطفال على الخط؟

☐ نعم

☐ لا

1.1.6 هل توجد تشريعات تتعلق بحماية الأطفال على الخط؟

الشرح: ~~*سيكون من الضروري عموماً أن توجد*~~ *يشير إلى مجموعة من القوانين التي توضح أن أي جريمة وكل جريمة ترتكب ضد أي طفل في العالم الحقيقي يمكن، مع إدخال ما يلزم من تغييرات، أن ترتكب على الإنترنت أو أي شبكة إلكترونية أخرى.* ~~*وقد يكون من الضروري أيضاً وضع قوانين جديدة أو تكييف القوانين*~~ *ويمكن أن يشير أيضاً إلى تشريعات لتجريم بعض أنواع السلوك التي لا يمكن أن تحدث إلا على الإنترنت، مثل إغراء الأطفال عن بُعد بأداء أو مشاهدة أفعال جنسية، أو "تجهيز" الأطفال لمقابلتهم في العالم الحقيقي لأغراض جنسية. (المبادئ التوجيهية للاتحاد من أجل واضعي السياسات بشأن حماية الأطفال على الخط).*

☐ نعم

☐ لا

☐ *جزئي (لا تكون إلا مسودات في مرحلة متقدمة وجاهزة للاعتماد أو التحقق منها)*

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

2.6 هل توجد وكالة/كيان مسؤول عن حماية الأطفال على الخط؟

الشرح: *وجود وكالة وطنية مخصصة لحماية الأطفال على الخط.*

☐ نعم

☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

1.2.6 هل هناك آلية عامة راسخة للإبلاغ عن القضايا المرتبطة بحماية الأطفال على الخط؟

الشرح: *رقم هاتف أو عنوان بريد إلكتروني أو موقع ويب يمكن للأطراف المعنية أن تبلغ من خلاله بالحوادث أو الشواغل المرتبطة بحماية الأطفال على الخط.*

☐ نعم

☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

2.2.6 هل هناك أي آليات أو إمكانات تقنية تستخدم في المساعدة على حماية الأطفال على الخط؟

☐ نعم

☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

3.2.6 هل توجد أي أنشطة تقوم بها مؤسسات حكومية أو غير حكومية لتوفير المعارف والدعم لأصحاب المصلحة بشأن كيفية حماية الأطفال على الخط؟

☐ نعم

☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

4.2.6 هل توجد برامج تثقيفية لحماية الأطفال على الخط؟

☐ للمعلمين

☐ للآباء

☐ للأطفال

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

3.6 هل توجد استراتيجية وطنية بشأن حماية الأطفال على الخط؟

☐ نعم

☐ لا

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

4.6 هل توجد حملات للوعي العام بشأن حماية الأطفال على الخط؟

☐ *للبالغين*

☐ *للشباب*

☐ *للأطفال*

يرجى تقديم روابط/محدد الموارد الموحد (URL)

يرجى تقديم الوثائق

7 إضافة: استقصاء قائم على الآراء

1.7 في رأيك، ما مدى أهمية زيادة الوعي بالأمن السيبراني كخطوة أساسية لتحقيق الأمن في الفضاء السيبراني؟

أ) ليس هاماً

ب) هام إلى درجة ما

ج) هام

د) هام جداً

2.7 ما هي المجموعات المستهدفة بحملات الوعي بالأمن السيبراني في بلدكم؟

أ)	الأطفال	ه)	الأشخاص ذوو الإعاقة
ب)	الشباب	و)	المؤسسات الخاصة
ج)	الطلبة	ز)	الوكالات الحكومية
د)	كبار السن	ح)	جهات أخرى

3.7 ما هي المجموعة الأكثر استهدافاً من بين هذه المجموعات؟ يرجى ترتيبها من 1 إلى 6 من أكثرها استهدافاً إلى أقلها استهدافاً.

أ)	الأطفال	ه)	الأشخاص ذوو الإعاقة
ب)	الشباب	و)	المؤسسات الخاصة
ج)	الطلبة	ز)	الوكالات الحكومية
د)	كبار السن	ح)	جهات أخرى

4.7 ما هي قضايا الأمن السيبراني التي تعالج في حملات التوعية الحالية؟ (يمكن الإجابة على أكثر من بند)

أ)	سلامة الإنترنت	ه)	البرمجيات الضارة
ب)	الخصوصية	و)	حماية الأطفال على الخط
ج)	التدليس	ز)	قضايا أخرى
د)	التصيّد		

5.7 ما هي درجة أهمية كل قضية؟ يرجى ترتيبها من أكثرها أهمية إلى أقلها أهمية وإعطاء أسباب الترتيب؟

أ)	سلامة الإنترنت	ه)	البرمجيات الضارة
ب)	الخصوصية	و)	حماية الأطفال على الخط
ج)	التدليس	ز)	قضايا أخرى
د)	التصيّد		

6.7 هل تتلقون أي مساعدة من الاتحاد أو تتعاونون معه في مجال الأمن السيبراني؟

أ) إذا كانت الإجابة نعم، يرجى ذكر التفاصيل ورأيك بشأن مدى فعالية هذه المساعدة/هذا التعاون واطلاعنا على المجالات المحددة بشأن الأمن السيبراني يتعين النظر فيها.

ب) إذا كانت الإجابة لا، كيف يمكننا المساعدة؟

_____