# دليل استبيان الرقم القياسي العالمي للأمن السيبراني (GCI) للعام 2016/2015

**هذه الوثيقة للعلم فقط.** تقيس الرقم القياسي العالمي للأمن السيبراني التزام البلدان في مجال الأمن السيبراني من خلال الدعائم 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 2016/2015 مع الأسئلة المطلوبة في المسألة 3 للجنة الدراسات 2 لقطاع تنمية الاتصالات. ويتألف الاستبيان من ثلاثة أقسام منفصلة، حيث تكون الإجابة على أسئلة القسمين الأول والثاني بنعم/لا فيما تكون الإجابة على أسئلة القسم الأخير مفتوحة بدون تحديد. 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.***

## القسم 1

## 1 هل توجد أي تشريعات ذات صلة بالمجال السيبراني؟

### 1.1 هل توجد أي قوانين للجريمة السيبرانية؟

**الشرح:** *أن تخصص تشريعات الجريمة السيبرانية قوانين بشأن النفاذ غير المصرّح به والتشويش أو التنصت على البيانات والأنظمة وإساءة استعمال أنظمة الحاسوب. ويشمل ذلك قانون الإجراءات وأي مواد موجودة بشأن الحفظ السريع للبيانات الحاسوبية المخزنة وأوامر الإنتاج وتجميع البيانات الحاسوبية في الوقت الفعلي وتسليم المتهمين والمساعدة المتبادلة والسرية والقيود المفروضة على الاستعمال؛ وإضافةً إلى السوابق القضائية بشأن الجريمة السيبرانية أو إساءة استعمال الحاسوب، يتعلق الأمر كذلك بأي جرائم تتعلق بالمحتوى. وقد تكون الأحكام جزءاً من قانون العقوبات وقانون حماية البيانات وقانون حرية المعلومات وتشريعات حقوق النشر/الملكية الفكرية.*

1.1.1 هل هناك قانون مستقل للجريمة السيبرانية؟

**الشرح:** *يشير مصطلح قانون مستقل إلى جميع فئات القانون العام والخاص، بما في ذلك قانون العقود وقانون العقارات وقانون الضرر وقانون الوصية والقانون الجنائي، التي تؤسس بشكل أساسي للحقوق وتحددها وتنظمها.*

1.1.1.1 هل هناك أي مواد بشأن النفاذ غير المخول إلى أجهزة الحاسوب والأنظمة والبيانات؟

**الشرح:** *يشير النفاذ غير المخول إلى الحصول على نفاذ إلى حاسوب أو نظام أو بيانات باستخدام حساب شخص آخر أو عن طريق وسائل غير شرعية بما في ذلك تخمين/استرجاع كلمات المرور وسرقة الهوية.*

2.1.1.1 هل هناك أي مواد بشأن التداخل/التعديل غير المخول على أجهزة الحاسوب والأنظمة والبيانات؟

**الشرح:** *يشير مصطلح التداخل/التعديل غير المخول إلى التطفل غير القانوني على نظام أو حاسوب أو بيانات الإجراء تغييرات على الحالة الأساسية لها وهو ما قد يتضمن إدخال بيانات حاسوبية أو الإضرار بها أو حذفها أو تغييرها بوجهٍ عام.*

3.1.1.1 هل هناك أي مواد بشأن الاعتراض غير المخول لأجهزة الحاسوب والأنظمة والبيانات؟

**الشرح:** *يشير مصطلح الاعتراض غير المخول إلى الالتقاط غير القانوني للإرسالات غير العمومية للبيانات الحاسوبية.*

2.1.1 هل توجد أي قوانين إجرائية للجريمة السيبرانية؟

**الشرح:** *القواعد التي تستمع من خلالها المحكمة وتحدد ماذا يحدث في الدعاوى القضائية المدنية أو الإجراءات الجنائية أو الإدارية. وتوضع هذه القواعد لكفالة التطبيق النزيه والمطابق للأصول القانونية أو العدالة الأساسية على جميع القضايا المرفوعة أمام المحكمة.*

1.2.1.1 هل هناك أي مواد عن الحفظ السريع للبيانات الحاسوبية المخزنة؟

**الشرح:** *حفظ البيانات التزام تفرضه سلطة حكومية على شخص أو منظمة يتطلب الحفظ الآمن لنوع معين من البيانات من الضياع أو التعديل لفترة زمنية محددة.*

2.2.1.1 هل هناك أي مواد بخصوص أوامر الإفصاح؟

**الشرح:** *أمر الإفصاح عبارة عن التزام تفرضه سلطة حكومية على شخص أو منظمة يقتضي تقديم نوع معين متاح من البيانات الحاسوبية إلى مسؤولي إنفاذ القانون في غضون فترة زمنية محددة.*

3.2.1.1 هل هناك أي مواد بخصوص البحث في البيانات الحاسوبية المخزنة والتحفظ عليها؟

**الشرح:** *تشير عملية البحث في البيانات الحاسوبية والتحفظ عليها إلى التدابير التي تشمل التدابير التشريعية، والتي تمكن السلطات من البحث في نظام حاسوب وفي بيانات حاسوبية مخزنة في أراضيها والنفاذ إليها.*

4.2.1.1 هل هناك أي مواد تتعلق بجمع البيانات الحاسوبية في الوقت الفعلي؟

**الشرح:** *جمع البيانات في الوقت الفعلي يشير إلى التدابير، بما في ذلك التدابير التشريعية التي تمكّن السلطات من جمع أو تسجيل بيانات حركة الاتصالات في الوقت الفعلي في الأراضي التابعة لها والتي ترسل بواسطة نظام حاسوبي.*

5.2.1.1 هل هناك أي مواد تتعلق بتسليم المجرمين السيبرانيين؟

**الشرح:** *تسليم المطلوبين هو إجراء تسلم بموجبه حكومة أو دولة، بناءً على طلب رسمي من حكومة أو دولة أخرى، بتسليم فرد منهم أو مدان بجريمة سيبرانية وقعت في الولاية القضائية الثانية إلى هذه الولاية القضائية.*

6.2.1.1 هل هناك مواد تتعلق بالمساعدة المتبادلة؟

**الشرح:** *اتفاق بين بلدين أو أكثر بغرض جمع وتبادل المعلومات سعياً إلى إنفاذ القانونين العام أو الجنائي.*

7.2.1.1 هل هناك أي مواد تتعلق بالسرية أو تقييد الاستعمال؟

**الشرح:** *قد يستعمل طرف ما البيانات شريطة الالتزام ببعض مواد السرية أو استعمالها في استعمال محدد متفق عليه.*

3.1.1 هل هناك سوابق قضائية بشأن الجريمة السيبرانية أو إساءة استعمال الحاسوب؟

**الشرح:** *قد تشمل الجرائم التي تندرج ضمن إساءة استعمال الحاسوب القرصنة والنفاذ غير المخول إلى الأنظمة الحاسوبية ونشر برمجيات خبيثة وضارة عن عمد (البرمجيات المؤذية). وقد يتضمن النفاذ غير المخول لتعديل الحواسيب تعديل البرمجيات والبيانات وتغيير كلمات المرور ومعلمات التشكيل لمنع الآخرين من النفاذ إلى الحاسوب والتداخل مع التشغيل العادي للنظام للإخلال به.*

## 2.1 هل هناك أي تشريعات أو لوائح للأمن السيبراني؟

**الشرح:** *اللوائح عبارة عن قواعد يستند إليها أو يقصد بها تنفيذ جزء محدد من التشريعات. تقوم بإنفاذ اللوائح عادةً الهيئات التنظيمية التي تشكل أو يوكل إليها تنفيذ أهداف أو أحكام أي تشريع. ومن هنا، فإن تنظيم الأمن السيبراني ينطوي على وضع مبادئ تلتزم بها الأطراف المعنية المختلفة، تنشأ وتشكل جزءاً من عملية تنفيذ القوانين التي تتعامل مع حماية البيانات والتبليغ عن الانتهاكات ومتطلبات منح الشهادات/التقييس في مجال الأمن السيبراني وتنفيذ تدابير الأمن السيبراني ومتطلبات مراجعة الأمن السيبراني وحماية الخصوصية وحماية الأطفال على الخط والتوقيعات الرقمية والمعاملات الإلكترونية ومسؤولية موردي خدمات الإنترنت.*

1.2.1 هل توجد أي تشريعات أو لوائح لحماية البيانات؟

**الشرح:** *لوائح تتعلق بحماية البيانات الشخصية والتجارية والحكومية من النفاذ غير المخول أو التعديل أو التدمير أو الاستعمال.*

2.2.1 هل توجد أي تشريعات لحماية الأنظمة والشبكات؟

**الشرح:** *تدابير قانونية مصممة لحماية الأنظمة والشبكات من التداخل الضار.*

3.2.1 هل توجد أي تشريعات أو لوائح للتبليغ عن الانتهاكات؟

**الشرح:** *قوانين أو لوائح التبليغ عن الانتهاكات هي تلك التي تلزم أي كيان يتعرض لانتهاك ما بإبلاغ السلطات وعملائه والأطراف الأخرى عن الانتهاك واتخاذ خطوات أخرى لعلاج الأضرار الناجمة عن الانتهاك. وتسنّ هذه القوانين عادةً استجابةً إلى العدد المتصاعد من الانتهاكات لقواعد بيانات المستهلكين التي تتضمن معلومات شخصية يمكن التعرف على هوية أصحابها من خلالها.*

1.3.2.1 بالنسبة للبيانات؟

**الشرح:** *قوانين التبليغ عن الانتهاكات المتعلقة بالبيانات.*

2.3.2.1 بالنسبة للأنظمة والشبكات؟

**الشرح:** *قوانين التبليغ عن الانتهاكات المتعلقة بالأنظمة والشبكات. وقد تشمل هذه القوانين معياراً لرعاية الأمن السيبراني أو متطلبات أساسية أخرى لحماية بيانات المستهلكين مثل التحفير.*

4.2.1 هل هناك أي تشريعات أو لوائح بخصوص منح الشهادات/التقييس بالنسبة للأمن السيبراني؟

**الشرح:** *تنظيم الأمن السيبراني من منظور منح الشهادات/التقييس يلزم الكيانات العاملة داخل أراضي أي بلد بالحصول على البعض أو الحد الأدنى من المتطلبات المتعلقة بالشهادات/التقييس. وقد تختلف هذه المتطلبات باختلاف القطاع المعني من الاقتصاد. وتشمل هذه المعايير، على سبيل الذكر وليس الحصر، المعايير الموضوعة من جانب الوكالات التالية: ISO و ITU و IETF و IEEE و ATIS و OASIS و 3GPP و 3GPP2 و IAB و ISOC و ISG و ISI و ETSI و ISF و RFC و ISA و IEC و NERC و NIST و FIPS و PCI DSS، إلخ.*

1.4.2.1 بالنسبة للقطاع العام؟

**الشرح:** *لوائح تشير إلى الشهادات/أعمال التقييس الإلزامية بالنسبة للأمن السيبراني في القطاع العام.*

2.4.2.1 بالنسبة للقطاع الخاص؟

**الشرح:** *لوائح تشير إلى الشهادات/أعمال التقييس الإلزامية بالنسبة للأمن السيبراني في القطاع الخاص.*

5.2.1 هل تلزم التشريعات أو اللوائح بتنفيذ تدابير للأمن السيبراني؟

**الشرح:** *قد تشمل تدابير الأمن السيبراني، على سبيل الذكر وليس الحصر، تدابير تقنية وتنظيمية مثل: جدران الحماية وقائمة للتحكم في النفاذ وتحديد أدوار ومسؤوليات أمنية والتأمين ضد الجرائم السيبرانية (خاص).*

1.5.2.1 بالنسبة للقطاع العام؟

2.5.2.1 بالنسبة لمشغلي البنى التحتية الحرجة؟

**الشرح:** *البنى التحتية الحرجة هي الأنظمة الرئيسية الحاسمة بالنسبة للسلامة والأمن والأمن الاقتصادي والصحة العامة للبلد. وقد تشمل هذه الأنظمة، على سبيل الذكر وليس الحصر، أنظمة الدفاع والشؤون المصرفية والمالية والاتصالات والنقل والصحة والطاقة وما إلى ذلك.*

3.5.2.1 بالنسبة للقطاع الخاص؟

6.2.1 هل تفرض التشريعات أو اللوائح مراجعات للأمن السيبراني؟

**الشرح:** *مراجعة الأمن السيبراني عبارة عن تقييم نظامي ودوري لأمن نظام المعلومات. وقد تشمل المراجعة النمطية تقييم زمن التشكيلة المادية للنظام والبيئة والبرمجيات وعمليات تداول المعلومات وممارسات المستعملين.*

1.6.2.1 بالنسبة للقطاع العام؟

2.6.2.1 بالنسبة لمشغلي البنى التحتية الحرجة؟

3.6.2.1 بالنسبة للقطاع الخاص؟

7.2.1 هل هناك تشريعات أو لوائح تتناول بالتفصيل حماية الخصوصية؟

**الشرح:** *الخصوصية في الإنترنت هي مستوى الخصوصية والأمن للبيانات الشخصية التي تنشر عبر الإنترنت. وهو مصطلح فضفاض يشير إلى مجموعة متنوعة من العوامل والتقنيات والتكنولوجيات التي تستخدم لحماية البيانات والاتصالات والأفضليات الحساسة والخاصة. ومن أمثلة هذه التشريعات قانون حماية البيانات.*

8.2.1 هل هناك أي تشريعات أو لوائح بخصوص التوقيعات الرقمية والمعاملات الإلكترونية؟

**الشرح:** *التوقيع الرقمي هو تقنية رياضية تستعمل للتحقق من استيقان وسلامة رسالة أو برمجية أو وثيقة إلكترونية. والمعاملة الإلكترونية هي عملية بيع أو شراء سلع أو خدمات سواء كانت بين شركات تجارية وأسر منزلية وأفراد وحكومات ومنظمات من القطاعين العام والخاص، تجري عبر شبكات حاسوبية؛ وتشمل الأمثلة على هذه النصوص التشريعية قانون التجارة الإلكترونية والقانون الخاص بالتوقيعات الإلكترونية وقانون المعاملات الإلكترونية، وما إلى ذلك، والتي قد تحتوي على تشريعات بشأن إنشاء إدارة لمراقبة سلطات منح الشهادات.*

9.2.1 هل هناك أي تشريعات أو لوائح بخصوص مساءلة ومسؤولية موردي خدمات الإنترنت؟

**الشرح:** *موردو خدمات الإنترنت مسؤولون عن انتهاكات حقوق النسخ الناتجة عن تصرفات مستعمليهم. والموردون ملزمون بإبلاغ الشرطة أو فريق الاستجابة للطوارئ الحاسوبية (CERT) أو أي وكالة/سلطة وطنية أخرى مسؤولة عن العمليات السيبرانية غير القانونية التي تصدر عن البنى التحتية الخاصة بهؤلاء الموردين، وهو شرط للمراقبة الاستباقية للشبكة.*

10.2.1 هل هناك أي تشريعات أو لوائح تتعلق بمحاصرة أو كبح جماح الرسائل الاقتحامية؟

## 3.1 هل يوجد تدريب على الأمن السيبراني لموظفي إنفاذ القانون وغيرهم من الفاعلين في المجال القضائي والقانوني؟

**الشرح:** *عملية رسمية لتثقيف العاملين في القطاع القانوني بشأن أمن الحاسوب.*

1.3.1 بالنسبة لإنفاذ القانون (ضباط الشرطة ووكالات الإنقاذ)؟

2.3.1 بالنسبة للفاعلين في المجال الفضائي والقانوني (القضاة ووكلاء النيابة ومحامو المحاكم العليا والمدّعون العموميون والمحامون والمساعدون القانونيون وغيرهم)؟

3.3.1 هل التدريب متكرر؟

**الشرح:** *يجرى التدريب بصورة دورية أو متكررة.*

# 2 هل لديكم أي تدابير تقنية؟

## 1.2 هل لديكم فريق للاستجابة للحوادث الحاسوبية (CIRT) أو فريق للاستجابة للحوادث الأمنية الحاسوبية (CSIRT) أو فريق للاستجابة للطوارئ الحاسوبية بمسؤولية وطنية (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. 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.*

1.1.2 هل لهذه الأفرقة ولاية حكومية؟

**الشرح:** *مدعومة بقرار من الحكومة أو تشكل جزءاً من الهياكل الحكومية.*

2.1.2 هل تجري هذه الأفرقة تمارين متكررة 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؟*

3.1.2 هل الأفرقة CIRT أو CSIRT أو CERT منضمة إلى منتدى أفرقة الأمن والاستجابة للحوادث (FIRST)؟

**الشرح**: *عضوية كاملة أو جهة اتصال بالمنتدى FIRST.*

4.1.2 هل الأفرقة CIRT أو CSIRT أو CERT منضمة إلى جمعية من الجمعيات الأخرى لأفرقة الاستجابة للطوارئ الحاسوبية (فريق CERT إقليمي)؟

**الشرح**: *أي علاقة رسمية أو غير رسمية مع أي فريق CERT آخر داخل أو خارج البلاد، جزء من أي فريق CERT إقليمي.*

## 2.2 هل هناك أي فريق CERT حكومي؟

**الشرح**: *الفريق CSIRT/CIRT/CERT الحكومي هو أي كيان يتعامل مع حوادث الأمن أو الأمن السيبراني الحاسوبية التي تؤثر فقط على المؤسسات الحكومية. فإلى جانب الخدمات التفاعلية، يمكنه أيضاً الانخراط في خدمات استباقية مثل تحليل مواطن الضعف وإجراء المراجعات الأمنية. وخلافاً للفريق CERT الوطني الذي يخدم القطاعين العام والخاص، على السواء، يقدم الفريق CERT الحكومي خدماته لجهات من القطاع العام فقط.*

## 3.2 هل هناك أي أفرقة CERT قطاعية؟

**الشرح**: *الفريق CSIRT/CIRT/CERT هو كيان يتعامل مع حوادث الأمن أو الأمن السيبراني الحاسوبية التي تؤثر على قطاع بعينه. وتشكل الأفرقة CERT القطاعية عادةً من أجل القطاعات الحساسة مثل الرعاية الصحية والمرافق العامة وخدمات الطوارئ والقطاع المالي. وخلافاً للفريق CERT الحكومي الذي يخدم القطاع العام، يقدم الفريق CERT القطاعي خدماته لهيئات من قطاع وحيد فقط.*

## 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)، و RFC، 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.*

1.4.2 بالنسبة للقطاع العام؟

2.4.2 بالنسبة للقطاع الخاص؟

## 5.2 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)، و CISSP، و SSCP، و CBK CSSLP، والتحليل الجنائي في مجال الأمن السيبراني (ISC²) و GIAC و GIAC GSSP (SANS) و CISM و CISA و CRISC (ISACA) والرابطة الصناعية لتكنولوجيا الحوسبة (CompTIA) و C|CISCO و CEH و ECSA و CHFI (مجلس المجموعة الأوروبية) و OSSTMM (ISECOM) و PCIP/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) و(IAPP) CIPP وABCP وCBCP و(DRI) MBCP وBCCP وBCCS وBCCE وDRCS و(BCM) DRCE وCIA وCCSA (معهد المراجعين الداخليين)، والرابطة الدولية لمديري المخاطر المتخصصين، ومعهد إدارة المشاريع (PMP)، إلخ.*

1.5.2 بالنسبة للقطاع العام؟

2.5.2 بالنسبة للقطاع الخاص؟

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

**7.2 هل هناك أدوات وتدابير تقنية معنية متعلقة بتوفير الأمن السيبراني، مثل برمجيات مكافحة الفيروسات والرسائل الاقتحامية، متاحة للأشخاص ذوي الإعاقة؟**

## 3 هل لديكم أي تدابير تنظيمية؟

### 1.3 هل توجد استراتيجية 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.*

1.1.3 هل الاستراتيجية الوطنية لديكم قائمة بذاتها؟

**الشرح:** *قد تكون الاستراتيجية الوطنية للأمن السيبراني موجودة في وثيقة منفصلة عن الاستراتيجية الوطنية للمعلومات أو التكنولوجيا أو الأمن.*

1.1.1.3 هل تتناول هذه الاستراتيجية القطاع الخاص؟

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

2.1.1.3 هل تتناول هذه الاستراتيجية القطاع العام؟

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

3.1.1.3 هل يوجد بها قسم يتعلق بحماية البنى التحتية الحرجة للمعلومات؟

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

4.1.1.3 هل توجد خارطة طريق للإدارة؟

**الشرح:** *تتضمن الاستراتيجية خارطة طريق بمعالم بارزة لتحقيق الاستراتيجية واستكمالها.*

5.1.1.3 هل تنقح الاستراتيجية بشكل متكرر؟

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

6.1.1.3 هل الاستراتيجية مفتوحة للمشاورات العامة؟

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

7.1.1.3 هل تتضمن الاستراتيجية خطة تعافي وطنية؟

**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.*

2.1.3 هل تدخل الاستراتيجية الوطنية للأمن السيبراني لديكم ضمن استراتيجية وطنية أخرى أوسع؟

1.2.1.3 هل يوجد بالاستراتيجية قسم بخصوص حماية البنى التحتية الحرجة للمعلومات؟

**الشرح**: *البنى التحتية الحرجة هي الأنظمة الرئيسية الحاسمة بالنسبة للسلامة والأمن والأمن الاقتصادي والصحة العامة للبلد. وقد تشمل هذه الأنظمة، على سبيل الذكر وليس الحصر، أنظمة الدفاع والشؤون المصرفية والمالية والاتصالات والنقل والصحة والطاقة وما إلى ذلك.*

2.2.1.3 هل توجد خارطة طريق لإدارة قسم الأمن السيبراني؟

3.1.3 هل تحدد الاستراتيجية الأولويات للقطاع العام؟

4.1.3 إذا كانت لا توجد استراتيجية للأمن السيبراني، هل يجري إعداد واحدة في الوقت الراهن؟

5.1.3 هل الاستراتيجية الموجودة أو التي قيد الإعداد تتضمن إجراءات تتعلق بالأشخاص ذوي الإعاقة؟

## 2.3 هل توجد جهة/وكالة وطنية مسؤولة عن الأمن السيبراني؟

**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.*

1.2.3 هل توجد وكالة مسؤولة عن حماية البنى التحتية الحرجة للمعلومات؟

2.2.3 هل توجد وكالة وطنية تعمل كجهة اتصال بالنسبة للقضايا المتعلقة بالرسائل الاقتحامية؟

## 3.3 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.*

1.3.3 هل تجرى تقييمات المخاطر دورياً؟

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

1.1.3.3 هل هناك علامة بارزة للأمن السيبراني لتقييم المخاطر؟

2.1.3.3 هل تخضع النتائج للقياس أو التقييم من أجل التحسينات في المستقبل؟

2.3.3 هل تجري مراجعات للأمن السيبراني بصورة متكررة؟

**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 ا لمادية للنظام والبيئة والبرمجيات وعمليات تداول المعلومات وممارسات المستعملين.*

1.2.3.3 هل هذه المراجعات إلزامية؟

**الشرح:** *تفرضها لوائح داخلية أو قطاعية أو توجبها معايير منح الشهادات ISO270001.*

## 4 هل لديكم أي أنشطة لبناء القدرات؟

### 1.4 هل توجد هيئة للتقييس داخل البلاد؟

**الشرح:** *التقييس مؤشر جيد على مستوى اكتمال التكنولوجيا، وظهور معايير جديدة في مجالات رئيسية يؤكد الأهمية الحيوية للمعايير. وعلى الرغم من أن الأمن السيبراني كان دائماً مسألة تتعلق بالأمن الوطني وتعالج بشكل مختلف في البلدان المختلفة، هناك نُهُج مشتركة تدعمها معايير معترف بها بصورة شائعة. وتشمل هذه المعايير، على سبيل الذكر وليس الحصر، المعايير التي وضعتها الوكالات التالية: المنظمة الدولية للتوحيد القياسي (ISO)، والاتحاد الدولي للاتصالات، وفريق مهام هندسة الإنترنت (IETF)، ومعهد المهندسين الكهربائيين والإلكترونيين (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. ويقيس هذا المؤشر وجود هيئة تقييس وطنية للأمن السيبراني والأنشطة الخاصة بوضع وتنفيذ معايير للأمن السيبراني.*

1.1.4 هل تقوم هذه الهيئة بوضع معايير الأمن السيبراني الخاصة بها؟

**الشرح:** *معايير الأمن السيبراني عبارة عن تقنيات توضع بشكل عام في صورة مواد منشورة تسعى إلى حماية البيئة السيبرانية لمستعمل أو منظمة. وتشمل هذه البيئة المستعملين أنفسهم والشبكات والأجهزة وجميع البرمجيات والعمليات والمعلومات المخزنة أو العابرة والتطبيقات والخدمات والأنظمة التي يمكن توصيلها بالشبكات بشكل مباشر أو غير مباشر. ويتمثل الهدف الأساسي في الحد من المخاطر، بما في ذلك منع هجمات الأمن السيبراني أو التخفيف من حدتها؛ وتعتمد بعض البلدان معايير دولية وتكيفها حسب بيئتها المحلية وتطلقها تحت مسمى معيار وطني. فيما تقوم بلدان أخرى (مع تقدم أنشطة البحث والتطوير) بوضع معايير تعتمد على قدر الاستعمال وتكتسب الاعتراف الدولي وتدخل ضمن معايير دولية جديدة.*

2.1.4 هل تعتمد هذه الهيئة معايير الأمن السيبراني الدولي القائمة؟

**الشرح:** *معايير الأمن السيبراني عبارة عن تقنيات توضع بشكل عام في صورة مواد منشورة تسعى إلى حماية البيئة السيبرانية لمستعمل أو منظمة. وتشمل هذه البيئة المستعملين أنفسهم والشبكات والأجهزة وجميع البرمجيات والعمليات والمعلومات المخزنة أو العابرة والتطبيقات والخدمات والأنظمة التي يمكن توصيلها بالشبكات بشكل مباشر أو غير مباشر. ويتمثل*

*الهدف الأساسي في الحد من المخاطر، بما في ذلك منع هجمات الأمن السيبراني أو التخفيف من حدتها؛ وتعتمد بعض البلدان معايير دولية وتكيفها حسب بيئتها المحلية وتطلقها تحت مسمى معيار وطني. فيما تقوم بلدان أخرى (مع تقدم أنشطة البحث والتطوير) بوضع معايير تعتمد على قدر الاستعمال وتكتسب الاعتراف الدولي وتدخل ضمن معايير دولية جديدة.*

### 2.4 هل تم تجميع أفضل ممارسات الأمن السيبراني الوطني أو القطاعية أو تم إعداد مبادئ توجيهية في هذا الصدد؟

**الشرح:** *أفضل الممارسات هي طرائق أو إجراءات لديها سجل مثبت بالنجاح. واعتماد أفضل الممارسات لن يقلل فقط من احتمال حدوث العطل، بل سيزيد من الكفاءة أيضاً.*

### 3.4 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.*

1.3.4 بالنسبة للقطاع العام؟

2.3.4 بالنسبة لمؤسسات التعليم العالي؟

3.3.4 هل هناك هيئة مؤسسة معترف بها وطنياً تشرف على أنشطة البحث والتطوير في مجال الأمن السيبراني؟

### 4.4 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.*

1.4.4 بالنسبة للمنظمات؟

**الشرح:** *حملات للوعي العام تستهدف المنظمات.*

2.4.4 بالنسبة للمجتمع المدني؟

**الشرح:** *حملات للوعي العام تستهدف الجمهور عامةً.*

1.2.4.4 للبالغين (أكبر من 18 عاماً)؟

2.2.4.4 للشباب (من 12 إلى 17 عاماً)؟

3.2.4.4 للأطفال (أقل من 12 عاماً)؟

3.4.4 في إطار حملات الوعي العام، هل يحاط الجمهور علماً بفوائد استعمال البرمجيات أو العتاد أو الحلول القائمة على الخدمة للأمن السيبراني؟

4.4.4 هل هناك أي من هذه البرمجيات أو العتاد أو الحلول القائمة على الخدمة متاح للجمهور؟

**الشرح:** *أن يتاح للجمهور بالمجان، على سبيل المثال، في إطار حملات التوعية أو تقوم برسوم مخفضة.*

### 5.4 هل تقوم منظمتكم/حكومتكم بوضع أي من مناهج التدريب المهني في مجال الأمن السيبراني أو تدعم وضع هذه المناهج؟

**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.*

1.5.4 بالنسبة للمنظمات؟

2.5.4 بالنسبة للقطاع العام؟

3.5.4 بالنسبة للقطاع الخاص؟

### 6.4 هل تقوم منظمتكم/حكومتكم بوضع أي برامج تعليمية أو مناهج أكاديمية في مجال الأمن السيبراني أو تدعم وضع هذه البرامج والمناهج؟

**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.*

1.6.4 في مدارس التعليم الأساسي؟

2.6.4 في المدارس الثانوية؟

3.6.4 في مؤسسات التعليم العالي؟

### 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.*

1.7.4 هل توجد هيئة مؤسسية معترف بها وطنياً للإشراف على أنشطة بناء القدرات في مجال الأمن السيبراني؟

### 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.*

1.8.4 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.*

1.1.8.4 هل تقدمون إعانات مالية للشركات التجارية والكيانات الأخرى غير القادرة على عمل تأمين ضد المخاطر السيبرانية في السوق المفتوحة؟

2.8.4 هل تقدم أي حوافز لتطوير صناعة للأمن السيبراني؟

**الشرح:** *يبحث هذا المؤشر 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.*

1.2.8.4 هل يقدم أي دعم للمشاريع المبتدئة في مجال الأمن السيبراني؟

**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).*

# 5 هل لديكم تدابير تعاونية؟

## 1.5 هل هناك أي اتفاقات ثنائية بشأن التعاون في مجال الأمن السيبراني؟

**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).*

1.1.5 مع الدول الوطنية؟

1.1.1.5 هل الاتفاق ملزم قانوناً؟

**الشرح:** *عبارة قانونية شائعة تشير إلى أن الاتفاق أُبرم بإرادة كاملة وأن هناك بعض الإجراءات التي يفرضها أو يحظرها القانون.*

1.1.1.1.5 بالنسبة لتبادل المعلومات؟

**الشرح:** *يشير مصطلح تبادل المعلومات إلى تبادل المعلومات المتعلقة بالتهديدات.*

2.1.1.1.5 بالنسبة لتبادل الأصول؟

**الشرح:** *يشير مصطلح تبادل الأصول إلى تبادل المهنيين (انتدابات أو إعارات أو غير ذلك من التكليفات المؤقتة للموظفين) والمرافق والمعدات والأدوات والخدمات الأخرى.*

2.1.1.5 هل الاتفاق غير ملزم قانوناً أو غير رسمي أو في انتظار التصديق؟

1.2.1.1.5 بالنسبة لتبادل المعلومات؟

2.2.1.1.5 بالنسبة لتبادل الأصول؟

**الشرح:** *قد تشمل الأصول موارد بشرية ومرافق ومعدات وما إلى ذلك.*

2.1.5 مع المنظمات الدولية؟

1.2.1.5 هل الاتفاق ملزم قانوناً؟

1.1.2.1.5 بالنسبة لتبادل المعلومات؟

2.1.2.1.5 بالنسبة لتبادل الأصول؟

**الشرح:** *قد تشمل الأصول موارد بشرية ومرافق ومعدات وما إلى ذلك.*

2.2.1.5 هل الاتفاق غير ملزم قانوناً أو غير رسمي أو في انتظار التصديق؟

1.2.2.1.5 بالنسبة لتبادل المعلومات؟

2.2.2.1.5 بالنسبة لتبادل الأصول؟

**الشرح:** *قد تشمل الأصول موارد بشرية ومرافق ومعدات وما إلى ذلك.*

## 2.5 هل توجد أي اتفاقات متعددة الأطراف أو دولية 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.*

1.2.5 هل الاتفاق ملزم قانوناً؟

1.1.2.5 بالنسبة لتبادل المعلومات؟

2.1.2.5 بالنسبة لتبادل الأصول؟

**الشرح:** *قد تشمل الأصول موارد بشرية ومرافق ومعدات وما إلى ذلك.*

2.2.5 هل الاتفاق غير ملزم قانوناً أو غير رسمي أو في انتظار التصديق؟

1.2.2.5 بالنسبة لتبادل المعلومات؟

2.2.2.5 بالنسبة لتبادل الأصول؟

**الشرح:** *قد تشمل الأصول موارد بشرية ومرافق ومعدات وما إلى ذلك.*

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

## 4.5 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.*

1.4.5 مع شركات محلية؟

1.1.4.5 بالنسبة لتبادل المعلومات؟

2.1.4.5 بالنسبة لتبادل الأصول؟

2.4.5 مع شركات أجنبية؟

1.2.4.5 بالنسبة لتبادل المعلومات؟

2.2.4.5 بالنسبة لتبادل الأصول؟

**الشرح:** *قد تشمل الأصول موارد بشرية ومرافق ومعدات وما إلى ذلك.*

## 5.5 هل توجد أي شراكات بين الوكالات؟

**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.*

1.5.5 بالنسبة لتبادل المعلومات؟

2.5.5 بالنسبة لتبادل الأصول؟

**الشرح:** *قد تشمل الأصول موارد بشرية ومرافق ومعدات وما إلى ذلك.*

## القسم 2

# 1 هل لديكم تدابير لحماية الأطفال على الخط؟

## 1.1 هل توجد تشريعات تتعلق بحماية الأطفال على الخط؟

**الشرح:** *سيكون من الضروري عموماً أن توجد مجموعة من القوانين التي توضح أن أي جريمة وكل جريمة ترتكَب ضد أي طفل في العالم الحقيقي يمكن، مع إدخال ما يلزم من تغييرات، أن ترتكب على ا لإنترنت أو أي شبكة إلكترونية أخرى. وقد يكون من الضروري أيضاً وضع قوانين جديدة أو تكييف القوانين الموجودة 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).*

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

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

1.2.1 هل هناك آلية عامة راسخة للإبلا غ 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.*

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

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

4.2.1 هل توجد برامج تثقيفية لحماية الأطفال على الخط؟

1.4.2.1 بالنسبة للمعلمين؟

2.4.2.1 بالنسبة للآباء؟

3.4.2.1 بالنسبة للأطفال؟

## 3.1 هل توجد استراتيجية وطنية بشأن حماية الأطفال على الخط؟

## 4.1 هل توجد حملات للوعي العام بشأن حماية الأطفال على الخط؟

1.1.4.1 من أجل البالغين (الأكبر من 18 عاماً)؟

2.1.4.1 من أجل الشباب (بين 12 و17 عاماً)؟

3.1.4.1 من أجل الأطفال (الأصغر من 12 عاماً)؟

## القسم 3

**إضافة: استقصاء قائم على الآراء؟**

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

أ ) الأطفال

ب) الشباب

ج) الطلبة

د ) كبار السن

هـ ) الأشخاص ذوو الإعاقة

و ) المؤسسات الخاصة

ز ) الوكالات الحكومية

ح) جهات أخرى

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

أ ) الأطفال

ب) الشباب

ج) الطلبة

د ) كبار السن

هـ ) الأشخاص ذوو الإعاقة

و ) المؤسسات الخاصة

ز ) الوكالات الحكومية

ح) جهات أخرى

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

أ ) سلامة الإنترنت

ب) الخصوصية

ج) التدليس

د ) التصيّد

هـ ) البرمجيات الضارة

و ) حماية الأطفال على الخط

ز ) قضايا أخرى

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

أ ) سلامة الإنترنت

ب) الخصوصية

ج) التدليس

د ) التصيّد

هـ ) البرمجيات الضارة

و ) حماية الأطفال على الخط

ز ) قضايا أخرى

6 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 وإطلاعنا إذا كانت هناك مجالات محددة بشأن الأمن السيبراني يتعين النظر فيها.

ب) إذا كانت الإجابة لا، يرجى إفادتنا كيف يمكننا المساعدة؟