



الهيئة الوطنية  
للأمن السيبراني  
National Cybersecurity Authority

# مشروع الإطار التنظيمي لترخيص تقديم خدمات ومنتجات وحلول الأمن السيبراني

Regulatory Framework for Licensing Cybersecurity Services, Products and  
Solutions  
(RFCS – 1: 2026)

إشارة المشاركة: شفاف

تصنيف الوثيقة: عام

بسم الله الرحمن الرحيم

مدىبات العموم

## بروتوكول الإشارة الضوئية (TLP):

يستخدم هذا البروتوكول على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

### أحمر (شخصي وسري للمستلم فقط)

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد، سواء أكان ذلك من داخل الجهة أم خارجها؛ خارج النطاق المحدد للاستلام.

### برتقالي + مشدد

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب.

### برتقالي (مشاركة محدودة)

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

### أخضر (مشاركة في نفس المجتمع)

المستلم يمكنه مشاركة المعلومات مع آخرين في الجهة نفسها، أو جهة أخرى على علاقة معهم أو في القطاع نفسه؛ ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

### شفاف (غير محدود)

معلومات

## الصفحة

## قائمة المحتويات

|    |  |    |
|----|--|----|
| ٤  | المقدمة  | ١  |
| 0  | التعريفات  | ٢  |
| ٦  | أهداف الإطار   | ٣  |
| ٦  | نطاق تطبيق الإطار  | ٤  |
| ٦  | مجالات التراخيص  | ٥  |
| ٧  | فئات التراخيص ومستوياتها   | ٦  |
| ١٠ | حوكمة تقديم خدمات أو منتجات أو طول الأمان السيبراني المرخصة  | ٧  |
| ١٠ | ٧,١ الاختصاصات والعمليات التي تقوم بها الهيئة باعتبارها الجهة المختصة بالأمن السيبراني في المملكة                                |    |
| ١٠ | ٧,٢ آلية تقديم الخدمات والمنتجات والطول الموضحة في فئة الترخيص المتخصص باستثناء خدمة الاستجابة والتحقيق في الحوادث السيبرانية... |    |
| ١١ | ٧,٣ آلية تقديم خدمة الاستجابة والتحقيق في الحوادث السيبرانية   |    |
| ١١ | أحكام التراخيص في فئة الترخيص المتخصص  | ٨  |
| ١١ | ٨,١ متطلبات الحصول على الترخيص في فئة الترخيص المتخصص  |    |
| ١٢ | ٨,٢ التزامات المرخص في فئة الترخيص المتخصص   |    |
| ١٣ | ٨,٢,١ الالتزامات العامة  |    |
| ١٤ | ٨,٢,٢ الالتزامات الخاصة بتقديم بعض الخدمات   |    |
| ١٧ | أحكام التراخيص في فئة الترخيص العام  | ٩  |
| ١٧ | ٩,١ متطلبات الحصول على الترخيص في فئة الترخيص العام  |    |
| ١٧ | ٩,٢ التزامات المرخص في فئة الترخيص العام   |    |
| ١٩ | طلب الحصول على الترخيص والمحافظة عليه وتجديده سواء من فئة الترخيص المتخصص أو فئة الترخيص العام                                   | ١٠ |
| ١٩ | التنازل عن الترخيص سواء من فئة الترخيص المتخصص أو فئة الترخيص العام  | ١١ |
| ٢٠ | إلغاء الترخيص وتعليقه سواء من فئة الترخيص المتخصص أو فئة الترخيص العام   | ١٢ |
| ٢٠ | التعاقد من الباطن  | ١٣ |
| ٢١ | أحكام عامة   | ١٤ |
| ٢٢ | الملاحق  | ١٥ |
| ٢٢ | الملاحق (أ): خدمات ومنتجات وطول الأمان السيبراني   |    |
| ٣٦ | الملاحق (ب): جدول المقابلات المالية لطلب ترخيص تقديم خدمات أو منتجات أو طول الأمان السيبراني                                     |    |

## ١. المقدمة

تُعد الهيئة الوطنية للأمن السيبراني؛ بموجب تنظيمها الصادر بالأمر الملكي الكريم رقم (٦٨٠١) في ١١/٢/١٤٣٩هـ الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه. وتهدف إلى تعزيزه؛ حمايةً للمصالح الحيوية للدولة، وأمنها الوطني، والبنى التحتية الحساسة، والقطاعات ذات الأولوية، والخدمات والأنشطة الحكومية. وتشمل اختصاصات الهيئة ومهامها وضع السياسات وآليات الحوكمة، والأطر، والمعايير، والضوابط، والإرشادات المتعلقة بالأمن السيبراني، وتعميمها على الجهات ذات العلاقة، ومتابعة الالتزام بها، وتحديثها، والترخيص بمزاولة الأفراد والجهات غير الحكومية، للأنشطة، والعمليات المتعلقة بالأمن السيبراني، التي تحددها الهيئة، وتحفيز نمو قطاع الأمن السيبراني في المملكة، وتشجيع الابتكار والاستثمار فيه.

وسعيًا من الهيئة الوطنية للأمن السيبراني لضمان تقديم خدمات ومنتجات وحلول الأمن السيبراني بأكبر قدر من الكفاءة والفاعلية والموثوقية في المملكة؛ للإسهام في تعزيز الأمن السيبراني على المستوى الوطني، والارتقاء بالخدمات المقدمة للجهات الوطنية، ونظرًا لأهمية تنظيم عمل سوق الأمن السيبراني في المملكة في سبيل إيجاد بيئة محفزة تعزز نمو قطاع الأمن السيبراني، فقد أصدرت الهيئة الوطنية للأمن السيبراني هذا الإطار؛ بهدف تنظيم عملية الترخيص لتقديم خدمات ومنتجات وحلول الأمن السيبراني في المملكة، والذي يبين المسؤوليات والالتزامات الواقعة على المرخص له، عند تقديم أي نوع من أنواع الخدمات؛ إضافة لتقديمها من جهات مؤهلة لذلك.

## ٢. التعريفات

يكون للمصطلحات المستخدمة في هذا الإطار المعاني المبينة أمام كل منها؛ ما لم يقتض السياق خلاف ذلك:

| المصطلح                 | المفهوم  |
|-------------------------|--|
| الهيئة                  | الهيئة الوطنية للأمن السيبراني.  |
| الأمن السيبراني         | حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.  |
| حصين                    | منظومة وطنية سيبرانية شاملة؛ تقدم الهيئة من خلالها خدمات ومنتجات سيبرانية مركزية، وغير مركزية، على المستوى الوطني للجهات المستفيدة (وهي الجهات الحكومية، وجهات البنية التحتية الوطنية الحساسة، والجهات الخاصة) بما يتوافق مع مهمات الهيئة واختصاصاتها، ومتطلباتها التنظيمية السيبرانية الوطنية.  |
| الإطار                  | الإطار التنظيمي لترخيص تقديم خدمات ومنتجات وحلول الأمن السيبراني، الصادر عن الهيئة.  |
| الترخيص                 | هو وثيقة تُصدرها الهيئة؛ تسمح بموجبه ممارسة نشاط تقديم خدمات ومنتجات وحلول الأمن السيبراني في المملكة؛ وذلك وفقاً لما تحدده الهيئة.  |
| شهادة التأهيل           | هي وثيقة تعتمدها الهيئة لشخص طبيعي، تقضي بأهليته للعمل في تقديم خدمات ومنتجات وحلول الأمن السيبراني في المملكة؛ وذلك وفقاً لما تحدده الهيئة.   |
| الفضاء السيبراني        | الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، التي تشمل الإنترنت، وشبكات الاتصالات، وأنظمة الحاسب الآلي، والأجهزة المتصلة بالإنترنت، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات.   |
| التهديد السيبراني       | أي ظرف أو حدث يمكن أن يؤثر سلباً على الشبكات أو أنظمة تقنية المعلومات أو أنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، سواء أكان ذلك التأثير باختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع.  |
| الثغرات السيبرانية      | ضعف في الشبكات أو أنظمة تقنية المعلومات أو أنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، قد يؤدي إلى اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع.  |
| الحادثة السيبرانية      | أي حدث يقع على الشبكات أو أنظمة تقنية المعلومات أو أنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، سواء أكان ذلك الحدث اختراقاً أو تعطيلاً، أو تعديلاً أو دخولاً أو استخداماً أو استغلالاً غير مشروع.  |
| الكيان                  | أي شخص طبيعي أو اعتباري يقدم أو يعتزم تقديم خدمات أو منتجات أو حلول متعلقة بالأمن السيبراني للجهات الوطنية في المملكة سواء أكان جهات عامة أو خاصة أو غيرها ويشمل ذلك أي جهة حكومية في المملكة العربية السعودية، والجهات والشركات التابعة لها، وجهات القطاع الخاص، التي تمتلك بنية تحتية وطنية حساسة، أو تقوم بتشغيلها، أو استضافتها، وغيرها من الجهات في القطاع الخاص، والجمعيات والمؤسسات الأهلية وغيرها. |
| الجهة الوطنية المستفيدة | هي الجهة التي تتعاقد مع كيان، بهدف الحصول على خدمات ومنتجات وحلول الأمن السيبراني في المملكة.  |

### ٣. أهداف الإطار

يهدف الإطار التنظيمي لترخيص تقديم خدمات ومنتجات وحلول الأمن السيبراني؛ إلى تنظيم تقديم هذه الخدمات والمنتجات والحلول في المملكة العربية السعودية من خلال إطار تنظيمي يحدد المسؤوليات والالتزامات على المرخص له؛ بما يسهم في تعزيز كفاءة وجودة تلك الخدمات والمنتجات والحلول أثناء تقديمها إلى الجهات المختلفة. ويمكن إيجاز الأهداف التي يسعى هذا الإطار إلى تحقيقها في الآتي:

١. الإسهام في تعزيز الأمن السيبراني في المملكة؛ من خلال تقديم خدمات ومنتجات وحلول الأمن السيبراني بجودة عالية، وفق متطلبات محددة.
٢. قيام الجهات الوطنية (العامة والخاصة وغيرها) في المملكة بمسؤوليتها تجاه أمنها السيبراني؛ والاستفادة من خدمات وحلول ومنتجات مرخصين من قبل الهيئة.
٣. تحفيز نمو قطاع الأمن السيبراني في المملكة، وتعزيز تنافسيته.
٤. تشجيع الابتكار، والاستثمار في قطاع الأمن السيبراني؛ من خلال دعم توفير خدمات ومنتجات مبتكرة تلبى الطلب المتزايد، في تقديم خدمات ومنتجات الأمن السيبراني.
٥. حماية حقوق كافة الأطراف ذات العلاقة بموجب هذا الإطار.
٦. تعزيز تنمية القدرات البشرية الوطنية، المتخصصة في تقديم خدمات ومنتجات وحلول الأمن السيبراني.

### ٤. نطاق تطبيق الإطار

ينطبق هذا الإطار على أي كيان يقدم أو يعتزم تقديم خدمات أو منتجات أو حلول متعلقة بالأمن السيبراني لجميع الجهات في المملكة، سواء من خلال التعاقد المباشر مع تلك الجهات، أو بشكل غير مباشر، مثل العمل مع أحد الكيانات الحاصلة على الترخيص بشكل غير مباشر. ويستثنى من ذلك ترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدار، حيث أن تنظيم ترخيص هذه الخدمة يتم وفق الإطار التنظيمي لترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدار.

### ٥. مجالات التراخيص

تم تحديد مجالات التراخيص بناءً على تصنيف خدمات ومنتجات الأمن السيبراني في المملكة، والذي يتضمن (٥) مجالات رئيسية، ينبثق منها (٢٥) مجال فرعي، وتتضمن تلك المجالات الفرعية عدة خدمات ومنتجات وحلول. ويوضح الشكل رقم (١) المجالات الرئيسية والفرعية لتصنيف خدمات ومنتجات وحلول الأمن السيبراني في المملكة، كما يتضمن الملحق (١) قائمة شاملة بكافة خدمات ومنتجات وحلول الأمن السيبراني حسب التصنيف الصادر عن الهيئة.

## تصنيف خدمات ومنتجات وطول الأمن السيبراني في المملكة

(يتضمن الملحق (١) قائمة شاملة بكافة الخدمات والمنتجات والطول)

| المجال الرئيسي | منتجات وطول الأمن السيبراني   | خدمات الأمن السيبراني الاحترافية               | خدمات التقني للأمن السيبراني      | الخدمات المدارة للأمن السيبراني                  | خدمات التدريب وبناء القدرات في الأمن السيبراني |
|----------------|-------------------------------|--|-----------------------------------|--|--|
| المجال الفرعي  | أمن الأجهزة الطرفية وإدارتها  | الاستشارات الإدارية في الأمن السيبراني         | تطوير منتجات وطول الأمن السيبراني | طول الأمن السيبراني كخدمة                        | التدريب في مجال الأمن السيبراني                |
|                | أمن الشبكات                   | الاستشارات التقنية في الأمن السيبراني          | تكاملاً أنظمة الأمن السيبراني     | الإسناد الخارجي للقوى العاملة في الأمن السيبراني | التوعية في مجال الأمن السيبراني                |
|                | أمن البيانات                  | تقييم الالتزام بالضوابط السيبرانية             |                                   | خدمات مركز عمليات الأمن السيبراني                | اختبارات وشهادات الأمن السيبراني               |
|                | أمن التطبيقات                 | تقييم المخاطر السيبرانية                       |                                   |  | الفعاليات والمسابقات في الأمن السيبراني        |
|                | إدارة هويات الدخول والصلاحيات | التقييمات الفنية في الأمن السيبراني            |                                   |  |  |
|                | الحوكمة والمخاطر والالتزام    | الاستجابة والتحقيق في الحوادث                  |                                   |  |  |
|                | حلول عمليات الأمن السيبراني   | خدمات برامج مكافأة اكتشاف الثغرات (Bug bounty) |                                   |  |  |
|                | أمن الحوسبة السحابية          |  |                                   |  |  |
|                | أمن الأنظمة الخاصة            |  |                                   |  |  |

الشكل رقم (١)

## ٦. فئات التراخيص ومستوياتها

بناءً على مجالات التراخيص المشار لها في القسم رقم (٥)، وتحديدًا المجالات الفرعية من التصنيف والمكونة من (٢٥) مجالاً فرعياً؛ سوف تصدر الهيئة (٤) أنواع من التراخيص وفق فئتين ومستويين كالآتي:

- **فئة الترخيص المتخصص:** الترخيص الذي يتطلب حصول الكيان عليه قبل الشروع في تقديم عدد من الخدمات المتخصصة في الأمن السيبراني ذات الحساسية العالية، ويوضح الشكل رقم (٢) أدناه المجالات الفرعية ضمن هذه الفئة. وسيتم إصدار مستويين ضمن هذه الفئة (متخصص-١ أو متخصص-٢)، حيث يمكن للمرخص في كل مستوى العمل مع شريحة محددة من الجهات.
- **فئة الترخيص العام:** الترخيص الذي يتطلب حصول الكيان عليه قبل الشروع في تقديم عدد من الخدمات أو المنتجات أو الحلول في الأمن السيبراني، ويوضح الشكل رقم (٢) أدناه المجالات الفرعية ضمن هذه الفئة. وسيتم إصدار مستويين في هذه الفئة (عام-١ أو عام-٢)، حيث يمكن للمرخص في كل مستوى العمل مع شريحة محددة من الجهات.



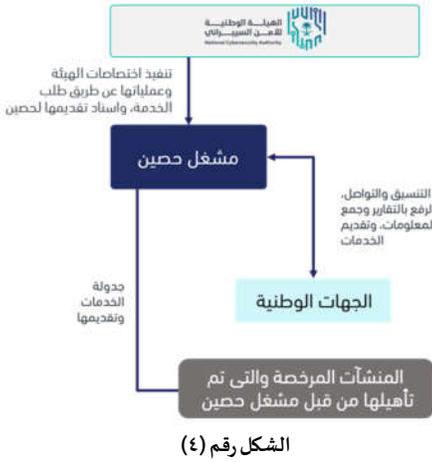
ويوضح الشكل رقم (٣) أدناه تفاصيل فئات التراخيص من حيث تعريف الفئة ومستوياتها:

| فئة الترخيص العام   | فئة الترخيص المتخصص   |
|---|---|
| الترخيص الذي يتطلب حصول الكيان عليه قبل الشروع في تقديم عدد من الخدمات أو المنتجات أو الحلول في الأمن السيبراني.  | الترخيص الذي يتطلب حصول الكيان عليه قبل الشروع في تقديم عدد من الخدمات المتخصصة في الأمن السيبراني ذات الحساسية العالية.  |
| المستوى الأول من فئة الترخيص العام<br>(عام - ١)   | المستوى الأول من فئة الترخيص المتخصص<br>(متخصص - ١)   |
| <p>تفاصيل الترخيص</p> <p>يمنح الترخيص (عام - ١) للكيانات المستوفية للأحكام الموضحة في القسم رقم (٩).</p> <p>يسمح للمرخص (عام - ١) العمل مع جميع الجهات الوطنية في المملكة؛ بما في ذلك الجهات الحكومية، والجهات التي تمتلك بنية تحتية حساسة، أو تقوم بتشغيلها، أو استضافتها؛ وذلك لتقديم الخدمات أو المنتجات أو الحلول المحددة في فئة الترخيص العام وفق ما هو موضح في الشكل رقم (٢).</p> <p>نطاق الترخيص</p> | <p>تفاصيل الترخيص</p> <p>يمنح الترخيص (متخصص - ١) للكيانات المستوفية للأحكام الموضحة في القسم رقم (٨).</p> <p>يسمح للمرخص (متخصص - ١) العمل مع جميع الجهات الوطنية في المملكة؛ بما في ذلك الجهات الحكومية، والجهات التي تمتلك بنية تحتية حساسة، أو تقوم بتشغيلها، أو استضافتها، وذلك لتقديم الخدمات المحددة في فئة الترخيص المتخصص وفق ما هو موضح في الشكل رقم (٢).</p> <p>نطاق الترخيص</p>   |
| المستوى الثاني من فئة الترخيص العام<br>(عام - ٢)  | المستوى الثاني من فئة الترخيص المتخصص<br>(متخصص - ٢)  |
| <p>تفاصيل الترخيص</p> <p>يمنح الترخيص (عام - ٢) للكيانات المستوفية للأحكام الموضحة في القسم رقم (٩).</p> <p>يسمح للمرخص (عام - ٢) العمل مع الجهات غير الحكومية، والجهات التي لا تمتلك بنية تحتية حساسة، أو تقوم بتشغيلها، أو استضافتها؛ وذلك لتقديم الخدمات أو المنتجات أو الحلول المحددة في فئة الترخيص العام وفق ما هو موضح في الشكل رقم (٢).</p> <p>نطاق الترخيص</p>                                     | <p>تفاصيل الترخيص</p> <p>يمنح الترخيص (متخصص - ٢) للكيانات المستوفية للأحكام الموضحة في القسم رقم (٨)؛ وتستثنى خدمات الاستجابة والتحقيق في الحوادث السيبرانية من الترخيص في هذا المستوى؛ حيث سيتم الترخيص لخدمات الاستجابة في المستوى الأول فقط.</p> <p>يسمح للمرخص (متخصص - ٢) العمل مع الجهات غير الحكومية، والجهات التي لا تمتلك بنية تحتية حساسة، أو تقوم بتشغيلها، أو استضافتها، وذلك لتقديم الخدمات المحددة في فئة الترخيص المتخصص وفق ما هو موضح في الشكل رقم (٢).</p> <p>نطاق الترخيص</p> |

الشكل رقم (٣)

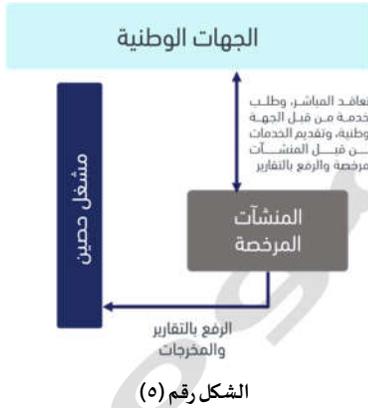
## ٧. حوكمة تقديم خدمات أو منتجات أو طول الأمن السيبراني المرخصة

### ٧,١ الاختصاصات والعمليات التي تقوم بها الهيئة باعتبارها الجهة المختصة بالأمن السيبراني في المملكة



لوفاء الهيئة الوطنية للأمن السيبراني بمهامها واختصاصاتها وفقاً لتنظيمها الصادر بالأمر الملكي الكريم ذي الرقم (٦٨٠١) في ١٤٣٩/٢/١١ هـ وذلك بهدف تعزيز الأمن السيبراني في المملكة حماية للمصالح الحيوية للدولة وأمنها الوطني؛ فإن الهيئة تقوم بتقديم عدد من خدمات الأمن السيبراني ذات الحساسية العالية بشكل مركزي ومباشر للجهات الوطنية (وبشكل خاص للجهات الحكومية، وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة أو تقوم بتشغيلها أو استضافتها). وتشمل تلك الخدمات إجراء تقييمات الالتزام بالضوابط والمعايير والأطر وغيرها من المتطلبات التنظيمية التي تصدرها الهيئة، وإجراء تقييمات مخاطر الأمن السيبراني، وإجراء التقييمات الفنية في الأمن السيبراني، وكذلك الاستجابة للحوادث السيبرانية وغيرها. ويوضح الشكل (٤) كيفية تقديم هذه الخدمات من خلال منظومة (حصين)، حيث تقوم الهيئة بتنفيذ اختصاصات ومهام مناهة بها عن طريق طلب الخدمة وإسناد تقديمها إلى مشغل (حصين)، والذي يتولى بدوره تنفيذ تلك الاختصاصات والمهام بالتنسيق مع الجهات الوطنية (العامة والخاصة وغيرها).

### ٧,٢ آلية تقديم الخدمات والمنتجات والحلول الموضحة في فئة الترخيص المتخصص باستثناء خدمات الاستجابة والتحقيق في الحوادث السيبرانية



لوفاء الجهات الوطنية بمسؤولياتهم تجاه أمنهم السيبراني، فإن ذلك قد يتطلب قيام الجهات الوطنية باتخاذ تدابير من شأنها رفع الجاهزية السيبرانية على مستوى الجهة والعمليات التشغيلية الداخلية، والتأكد من الالتزام الكامل والمستمر للسياسات وآليات الحوكمة والأطر والمعايير والضوابط والإرشادات وغيرها المتعلقة بالأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني، ومن ذلك على سبيل المثال إجراء تقييمات تحضيرية واسترشادية قبل التقييم الرسمي الذي تجريه الهيئة من خلال منظومة (حصين)، أو التقييمات التي يتم إجراؤها قبل إطلاق الخدمات الإلكترونية، ويشمل ذلك إجراء تقييمات الالتزام، أو التقييمات الفنية، أو تقييمات مخاطر الأمن السيبراني، وغيرها. وفي حال الحاجة لذلك، فيمكن للجهات الوطنية (العامة والخاصة وغيرها) التعاقد مع أحد المرخصين في فئة الترخيص المتخصص حسب المستوى الحاصل عليه المرخص؛ لتنفيذ تلك الخدمات. ويلتزم المرخص بتزويد الهيئة بجميع الوثائق والمعلومات والبيانات ذات الصلة بما يتم تقديمه من خدمات، وكذلك مخرجات ونتائج تنفيذ الخدمات من خلال منظومة (حصين) وفقاً للنماذج المعتمدة في هذا الشأن. ويجب على جميع المرخصين إطلاع منظومة (حصين) بجميع النشاطات التي تتم قبل تقديم الخدمة، وأثنائها، وبعدها. ويوضح الشكل (٥) كيفية تقديم هذه الخدمات.

## ٧,٣ آلية تقديم خدمات الاستجابة والتحقيق في الحوادث السيبرانية

في حال اشتباه أي جهة وطنية (عامة أو خاصة أو غيرها) بوقوع حادثة سيبرانية أو رصدتها لحادثة سيبرانية؛ فيجب أن تقوم بالإبلاغ فوراً عنها عبر منصة (حصين) أو من خلال القنوات المعتمدة من الهيئة في هذا الشأن بما في ذلك من خلال الرقم (٩٣٦). حيث سيتم تصنيف الحادثة السيبرانية وتحديد أولوية التعامل معها (Triage Process) من خلال منظومة (حصين)، ومن ثم التوجيه بإكمال الإجراءات اللازمة حسب الآتي:

أ. في حال تم تصنيف الحادثة السيبرانية على أنها من المستوى الأول أو الثاني أو الثالث، سيتم من خلال منظومة (حصين) الاستجابة للحادثة السيبرانية بشكل مباشر مع الجهة الوطنية (العامة أو الخاصة أو غيرها).

ب. في حال تم تصنيف الحادثة السيبرانية على أنها من المستوى الرابع أو الخامس، فسيقوم المرخص لتقديم خدمات مركز عمليات الأمن السيبراني المدار بتقديم الدعم اللازم للتعامل مع الحادثة وفقاً للالتزامات الترخيص الحاصل عليه، ويمكن للجهة الوطنية (العامة أو الخاصة أو غيرها) الاستعانة بأحد المرخصين لتقديم خدمات الاستجابة للحوادث عند الحاجة، والذي بدوره سيقوم بتقديم الخدمات. ويلتزم المرخص بإبرام اتفاقية مع مشغل (حصين) بهذا الشأن، والعمل وفق المنهجية التي تضعها منظومة (حصين) كما يعد المرخص ملزم بتزويد الهيئة بجميع الوثائق والمعلومات والبيانات ذات الصلة، وكذلك مخرجات الخدمات من خلال منظومة (حصين) وفقاً للنماذج المعتمدة في هذا الشأن. ويجب على جميع المرخصين إطلاع منظومة (حصين) بجميع النشاطات التي تتم قبل تقديم الخدمة، وأثناءها، وبعدها. وتحتفظ الهيئة وفق تقديرها بالحق بالإستجابة للحادثة بنفسها من المستوى الرابع أو الخامس حسب الاقتضاء.

## ٨. أحكام التراخيص ضمن فئة الترخيص المتخصص<sup>١</sup>

### ٨,١ متطلبات الحصول على الترخيص ضمن فئة الترخيص المتخصص

يجب على الكيان الذي يرغب بالحصول على ترخيص من المستوى الأول، أو المستوى الثاني لتقديم أي من خدمات الأمن السيبراني المحددة في فئة الترخيص المتخصص الموضحة في القسم رقم (٦) من هذه الوثيقة، استيفاء متطلبات الحصول على الترخيص وتجديده، والمحافظة عليه، وفق الجدول الآتي:

| المتطلبات العامة   |  | تصنيف المتطلبات     |
|--|--|---------------------|
| متطلبات المستوى الثاني من الترخيص المتخصص (٢ - متخصص)  | متطلبات المستوى الأول من الترخيص المتخصص (١ - متخصص) |                     |
| <ul style="list-style-type: none"><li>• أن يكون طالب الترخيص كيان؛ مؤسس بشكل نظامي في المملكة.</li><li>• تعبئة وتقديم نموذج طلب الترخيص.</li><li>• تقديم بيانات ملكية الكيان (المباشرة وغير المباشرة)، والمعلومات ذات الصلة (النظام الأساس، وعقد التأسيس، والسجل التجاري، وقائمة بجميع المسيطرين بما يبين عددهم ونسبة الملكية التي يمتلكها كل منهم) والهيكل التنظيمي للكيان، ونسبة التوطين للمناصب القيادية.</li></ul> |  | المتطلبات التنظيمية |

<sup>١</sup> يستثنى من ذلك ترخيص تقديم خدمات مركز عمليات الأمن السيبراني المدار، حيث أن تنظيم هذه الخدمة موضح في الإطار التنظيمي لترخيص تقديم خدمات مركز عمليات الأمن السيبراني المدار.

|   |  |                                      |
|---|--|--------------------------------------|
| <ul style="list-style-type: none"> <li>• تزويد الهيئة ببيانات الكيان (وثيقة العنوان الوطني، وغودج تعيين ممثل رسمي للكيان موقع ومختوم ومصدق من الغرفة التجارية، ووثيقة تسجيل استثمار أجنبي من وزارة الاستثمار في حال وجود ملكية أجنبية للجهة).</li> <li>• أن يكون نشاط الأمن السيبراني أحد الأنشطة الرئيسية للكيان.</li> </ul>   |  |                                      |
| <ul style="list-style-type: none"> <li>• أن تكون ملكية المواطن أو المواطنين السعوديين للحصص أو الأسهم حسب الأحوال (سواء أكانت ملكية مباشرة، أم غير مباشرة، من خلال شركات - مؤسسة بشكل نظامي في المملكة - مملوكة كلياً، أو جزئياً لمواطن أو أكثر) في الكيان طالب الترخيص، لا تقل عن نسبة ٢٥٪.</li> <li>• يتطلب هذا المستوى أن يتوفر لدى الكيان مستوى مناسب من القدرات التقنية والكفاءة التشغيلية، والقدرة على الالتزام بشروط تقديم الخدمات، وأن يتوفر لدى الكيان نضج مناسب سواءً في العمليات التي يتم تنفيذها، أو في مستوى الأمن السيبراني للكيان، وقدرة الكيان على ضمان الجودة والاستمرارية التشغيلية.</li> </ul> | <ul style="list-style-type: none"> <li>• أن تكون ملكية المواطن أو المواطنين السعوديين للحصص أو الأسهم حسب الأحوال (سواء أكانت ملكية مباشرة، أم غير مباشرة، من خلال شركات - مؤسسة بشكل نظامي في المملكة - مملوكة كلياً، أو جزئياً لمواطن أو أكثر) في الكيان طالب الترخيص، لا تقل عن نسبة ٧٥٪.</li> <li>• يتطلب أن يكون الكيان على قدر عالي من القدرات التقنية والكفاءة التشغيلية، والقدرة على الالتزام بشروط تقديم الخدمات، وأن يتوفر لدى الكيان نضج عالي سواءً في العمليات التي يتم تنفيذها، أو في مستوى الأمن السيبراني للكيان، وقدرة الكيان على ضمان الجودة والاستمرارية التشغيلية.</li> </ul> | <p>متطلبات خاصة بالكيان</p>          |
| <ul style="list-style-type: none"> <li>• يشترط ألا يقل رأس مال الكيان الراغب في الحصول على ترخيص في فئة الترخيص المتخصص من المستوى الثاني عن (٥٠٠) خمسمائة ألف ريال.</li> </ul>   | <ul style="list-style-type: none"> <li>• يشترط ألا يقل رأس مال الكيان الراغب في الحصول على ترخيص في فئة الترخيص المتخصص من المستوى الأول عن (١٠) عشرة ملايين ريال.</li> </ul>  | <p>رأس المال</p>                     |
| <ul style="list-style-type: none"> <li>• تقديم خطة العمل التقديرية/الأولية لتقديم الخدمات، مع بيان عدد العاملين لكل خدمة من الخدمات والآلية التي سيتم تبنيها لتقديم هذه الخدمات.</li> <li>• اجتياز الكيان لمتطلبات التأهيل اللازمة من منظومة حصين، بما في ذلك اجتياز التقييم الفني وتقييم الالتزام بمتطلبات الأمن السيبراني الصادرة عن الهيئة، التي تنطبق على المرخص وفقاً للتعليمات والمتطلبات التي تحددها الهيئة.</li> </ul>  |  | <p>المتطلبات الفنية</p>              |
| <p>يجب على الكيان الفصل ما بين الفرق بما يضمن تجنب تضارب المصالح.</p>   |  | <p>الفصل الوظيفي أو توزيع المهام</p> |
| <p>أن يتم تقديم الخدمات من قبل كوادر مؤهلين وذوي خبرة من الحاصلين على شهادة تأهيل، وفق ما يتم تحديده من قبل الهيئة.</p>   |  | <p>الكوادر المؤهلة</p>               |

## ٨,٢ التزامات المرخص في فئة الترخيص المتخصص

## ٨,٢,١ الالتزامات العامة

يجب على المرخص في كل الأحوال الالتزام بأحكام هذا الإطار، والقرارات، والتنظيمات، والأطر والضوابط والمعايير، والتعليمات، والتوجيهات، والتعاميم، وما في حكمها؛ الصادرة عن الهيئة. كما يجب عليه الالتزام بما يلي:

- ٨,٢,١,١ الأنظمة واللوائح، والتنظيمات، والتعليمات، المعمول بها في المملكة العربية السعودية.
- ٨,٢,١,٢ البدء بتقديم الخدمات المرخص بها خلال (٣) أشهر من تاريخ إصدار الترخيص في الحد الأقصى؛ ما لم تقرر الهيئة خلاف ذلك.
- ٨,٢,١,٣ التقيّد بمتطلبات التوطين، وإبقاء جميع المعلومات والبيانات المرتبطة بهذه الخدمات قبل أو أثناء أو بعد تقديمها لديه داخل المملكة العربية السعودية، وعدم تخزينها أو وضع نسخها منها خارج المملكة.
- ٨,٢,١,٤ تنفيذ الخدمات التي يتم الترخيص لها، وتقديمها للجهات الوطنية (العامة أو الخاصة أو غيرها) من داخل المملكة.
- ٨,٢,١,٥ أن تكون معالجة البيانات المتعلقة بالخدمات وتخزينها، داخل المملكة، وعدم السماح بالدخول عليها من خارج المملكة.
- ٨,٢,١,٦ التقيّد بالمنهجيات التي تضعها منظومة (حصين) لتقديم الخدمات، والالتزام بتزويد الهيئة بجميع الوثائق والمعلومات والبيانات ذات الصلة، وكذلك مخرجات الخدمات من خلال منصة (حصين) وخلال المدة المقررة لذلك.
- ٨,٢,١,٧ الالتزام بالمسؤوليات والواجبات عند تقديم الخدمات للجهات الوطنية، وفق ما يصدر من الهيئة.
- ٨,٢,١,٨ تنفيذ ما تجري مشاركته من الهيئة من توصيات أو متطلبات سيرانية وأمنية؛ بما في ذلك التنبيهات السيبرانية، وقواعد رصد التهديدات، ومؤشرات الاختراق. وتزويد الهيئة بالنتائج، وفق المتطلبات، والمدة المقررة منها.
- ٨,٢,١,٩ تزويد الهيئة بالتقارير الدورية - وفق ما تقرره - وأي معلومات أخرى تطلبها، والتقيّد بالمدد الزمنية ذات الصلة، والكيفية والنماذج المقررة لذلك، وتشمل التقارير - على سبيل المثال لا الحصر - التقييمات السيبرانية التي تم إجراؤها، وكذلك الحوادث السيبرانية التي جرى احتواؤها؛ والجهات الوطنية المستفيدة، وغيرها.
- ٨,٢,١,١٠ عدم نشر أي بيانات متعلقة بالأمن السيبراني، والمعلومات ذات الصلة التي حصل عليها المرخص نظير تقديم خدماته للجهات الوطنية (العامة أو الخاصة أو غيرها) في المملكة، قبل الحصول على موافقة خطية من الهيئة.
- ٨,٢,١,١١ عدم نشر و/ أو مشاركة أي بيانات للجهات الوطنية (العامة أو الخاصة أو غيرها) التي يعمل معها المرخص سواء بشكل منفرد أو بعد تجميع تلك البيانات أو المعلومات، مع أي جهة؛ بأي مسوغ، ولأي مسوغ بما فيها الجهات الحكومية أو الخاصة، داخل المملكة وخارجها؛ ويكون نشرها مشروطاً بموافقة خطية من الهيئة.
- ٨,٢,١,١٢ النص في تعاقده، ذات الصلة بهذا الإطار على الأحكام التي تعالج حالات انتهاء الترخيص، أو عدم تجديده، أو إلغائه.
- ٨,٢,١,١٣ تطبيق الإجراءات اللازمة، في حال انتهاء العلاقة التعاقدية أو إنهاؤها، مع الجهات الوطنية (العامة أو الخاصة أو غيرها)، وفق ما تقرره الهيئة.
- ٨,٢,١,١٤ عندما تجري الاستعانة بخدمات أحد مقدمي خدمات الحوسبة السحابية (CSP) فإنه يجب أن يجري التعاقد مع مقدم خدمات حوسبة سحابية مرخص من قبل الجهة المختصة في المملكة.
- ٨,٢,١,١٥ إبلاغ الهيئة فوراً بأي تغيير في المعلومات، أو البيانات ذات الصلة بطلب الترخيص و/ أو عند اكتشاف أي معلومات غير دقيقة أو مخالفة للواقع، لما جرى إبلاغ الهيئة بها، مع بيان الأسباب التي دعت لتقديمها بشكل غير دقيق، أو غير صحيح، وسبب التغيير فيها.
- ٨,٢,١,١٦ إبلاغ الهيئة - بشكل فوري - بأي خطر أو تهديد أو اختراق يرصده المرخص لدى الجهة الوطنية (العامة أو الخاصة أو غيرها)، سواء أكان ذلك واقعاً أو محتملاً.

- ٨,٢,١,١٧ إبلاغ الهيئة فوراً بأي إجراء قانوني أو تنظيمي ضده قد يؤثر على تقديم الخدمات؛ بغض النظر عن الجهة التنظيمية أو الاختصاص، وسواء أكان من داخل المملكة أم كان خارجها.
- ٨,٢,١,١٨ تقديم قوائم مالية مدققة من مراجع حسابات مستقل -مرخص بشكل نظامي، وفقاً لأنظمة المملكة- تظهر الإيرادات من تقديم خدمات أو منتجات أو حلول الأمن السيبراني لكل سنة مالية طوال فترة الترخيص.
- ٨,٢,١,١٩ التعاون التام مع الهيئة عند مباشرة اختصاصاتها التنظيمية والرقابية عليه بوصفه مرخص له، وإتاحة جميع الموارد الممكنة الخاصة به، لتنفيذ أي متطلبات للرقابة، والتفتيش من الهيئة، بما يشمل المراجعة والتحقق، وإجراء التقييمات السيبرانية، وأي متطلب آخر على أعماله وأنظمتها أي كانت.
- ٨,٢,١,٢٠ تزويد الهيئة بجميع الوثائق، والبيانات، والمعلومات، والتقارير، التي تثبت التزامه بتنظيمات الهيئة ومتطلباتها، وتشمل -دون حصر- ما يلي:
- ٨,٢,١,٢٠,١ معلومات الأداء المالي لأنشطة الأمن السيبراني، بما في ذلك الإيرادات ومصادرها، ورأس المال، والاستثمارات التقنية، واستثمارات البنية التحتية، ونفقات التدريب والتطوير.
- ٨,٢,١,٢٠,٢ معلومات خدمات الأمن السيبراني المقدمة، والجهات المتعاقد معها، وأسماء تلك الجهات وعددها، ونوع الخدمات المقدمة لها، والاجتماعات والتعاملات معها، وغير ذلك.
- ٨,٢,١,٢٠,٣ معلومات العاملين لديه المعنيين بتقديم الخدمات ضمن فئة الترخيص المتخصص، وغيرها من الخدمات حسب ما تراه الهيئة، على أن تشمل المعلومات عدد الموظفين، وبيانات السير الذاتية، والمؤهلات الخاصة بهم، وغير ذلك مما له علاقة بطبيعة العمل.
- ٨,٢,١,٢٠,٤ معلومات المتطلبات الفنية المفروضة على المرخص، والأدوات والاشتراكات التقنية، وأي بنية تحتية لتقنية المعلومات؛ لها صلة بتنفيذ خدمات الأمن السيبراني التي يتم تقديمها من قبل الكيان المرخص، وغير ذلك.
- ٨,٢,١,٢٠,٥ أي دليل أو وثيقة، أو مستند، أو إثبات تطلبه الهيئة، للتحقق من التزام المرخص بالأحكام الواردة في هذا الإطار، والوثائق الأخرى الصادرة عن الهيئة، وغيرها من الجهات المعنية.
- ٨,٢,١,٢١ الالتزام بنسب المحتوى المحلي على مستوى الكيان، والتوظيف للوظائف من الكفاءات الوطنية؛ وفق ما تقره الهيئة، والجهات المختصة.
- ٨,٢,١,٢٢ الالتزام بالقرارات والتعليمات الصادرة عن الهيئة، بما في ذلك تلك المتعلقة بأي خلافات قد تنشأ مع الجهة المتعاقد معها، تجاه الخدمات المقدمة بموجب الترخيص.
- ٨,٢,١,٢٣ التطبيق الكامل والمستمر لجميع ضوابط الأمن السيبراني الصادرة عن الهيئة، التي تنطبق على المرخص؛ وتشمل -دون حصر- الضوابط الأساسية للأمن السيبراني، وضوابط الأمن السيبراني لأنظمة الحساسة، وضوابط الأمن السيبراني للبيانات، وتقديم وثائق سنوية تثبت الالتزام بالضوابط الصادرة من قبل الهيئة.
- ٨,٢,١,٢٤ الالتزام بإشعار الهيئة فوراً عندما يطرأ أي تغيير في ملكية الكيان المرخص، بأي شكل كان.
- ٨,٢,١,٢٥ الالتزام بالحصول على موافقة الهيئة، الخطية المسبقة؛ قبل ترتيب أي إجراء من شأنه تحقيق تغيير في ملكية الكيان المرخص، بأي شكل كان.

## ٨,٢,٢ الالتزامات الخاصة

- ٨,٢,٢,١ الالتزامات الخاصة بتقديم خدمات تقييم الالتزام بالضوابط السيبرانية، وتقييم المخاطر السيبرانية، والتقييمات الفنية في الأمن السيبراني

- ٨,٢,٢,١,١ على المرخص إجراء التقييمات وفق آلية محددة وممنهجة على أن تتضمن الآلية صياغة تقرير نهائي شامل للتقييمات بأنواعها وفق منهجيات ومماذج منظومة (حصين)، وإرساله من خلال منصة (حصين) بالصيغة التي تحددها الهيئة وخلال المدة المقررة لذلك.
- ٨,٢,٢,١,٢ على المرخص اتباع منهجيات واضحة لإجراء تقييمات الالتزام على أن تتضمن المعايير الخاصة بالأدلة المسموح بها، والمعايير التي تحدد أداء الجهة الخاضعة للتقييم في مجال التقييم؛ وتحفظ الهيئة بحقوقها في تحديد آلية التقييم، ومنهجيتها ومحتوياتها بالكامل، وكذلك بحقوقها في إدخال أي تعديلات أو حذف أي من عناصرها.
- ٨,٢,٢,١,٣ على المرخص إجراء التقييمات من خلال كوادرات سعودية مؤهلة وذوي خبرة من الحاصلين على شهادة تأهيل، حيث يجب أن تكون هذه الكوادرات حاصلة على مؤهلات علمية وشهادات في مجال الأمن السيبراني أو المجالات ذات العلاقة، وأن تكون كوادرات ذات خبرة في مجال التقييمات، وذلك حسب ما يتم تحديده من قبل الهيئة.
- ٨,٢,٢,١,٤ على المرخص الاحتفاظ بسجلات دقيقة وكاملة عن التقييمات التي تم تقديمها للجهات الوطنية المستفيدة، لمدة (٥) سنوات من تاريخ تقديم تلك الخدمات؛ على أن تشمل - على سبيل المثال لا الحصر - تاريخ تقديم الخدمة، واسم الجهة المستفيدة من الخدمة، وبيانات العاملين الذين شاركوا في تقديم الخدمة، ونتائج التقييم بشكل مفصل، وأي طرف ثالث له علاقة في تقديم أي جزء من خدمات التقييمات.
- ٨,٢,٢,٢ الالتزامات الخاصة بتقديم خدمات برامج مكافأة اكتشاف الثغرات (Bug Bounty)**
- ٨,٢,٢,٢,١ اقتصر المشاركين في برامج مكافأة اكتشاف الثغرات على مواطنين ومقيمين في المملكة مستوفين الاشتراطات اللازمة.
- ٨,٢,٢,٢,٢ اقتصر نطاق البرامج على الأصول التي لا يُحتمل أن تؤثر على الأمن الوطني، والأصول ذات الواجهات العامة، وأن يستثني البرنامج الأنظمة التشغيلية والهندسة الاجتماعية.
- ٨,٢,٢,٢,٣ احتواء منصات برامج مكافأة اكتشاف الثغرات على المميزات الآتية: (١) إحصاءات وتتبع مباشر للنشاطات التي تتم ضمن المنصة، مثل متوسط وقت الحل، وعدد المكافآت المدفوعة، والثغرات المكتشفة وعددها. (٢) تحكم الجهات المشاركة في اختيار الباحثين المشاركين. (٣) إمكانية إصدار التقارير والبيانات للجهات.
- ٨,٢,٢,٢,٤ التحقق من هويات المستخدمين للمنصة، والاحتفاظ بسجلات المنصة لمدة (٥) سنوات على الأقل.
- ٨,٢,٢,٢,٥ إعطاء الهيئة الوطنية للأمن السيبراني صلاحية الاطلاع على معلومات وبيانات منصات برامج مكافأة اكتشاف الثغرات بشكل مباشر.
- ٨,٢,٢,٢,٦ أخذ الموافقة وتوقيع اتفاقية عدم الإفصاح بين الباحثين والمشاركين في المنصة من الجهات قبل تقديم الخدمة.
- ٨,٢,٢,٢,٧ أن تخضع سياسة الخصوصية على منصة برامج مكافأة اكتشاف الثغرات (Bug Bounty) لسياسات حوكمة البيانات الوطنية الصادرة من الجهة المختصة في المملكة ونظام حماية البيانات الشخصية والتشريعات ذات الصلة في المملكة.
- ٨,٢,٢,٣ الالتزامات الخاصة بتقديم خدمات الاستجابة والتحقيق في الحوادث السيبرانية (يتم ترخيص هذه الخدمة لمستوى واحد فقط، المستوى الأول من فئة الترخيص المتخصص (متخصص-١))**
- ٨,٢,٢,٣,١ على المرخص تحديد اتفاقية مستوى تقديم خدمة (SLA) واضحة مع الجهات الوطنية (العامة أو الخاصة أو غيرها).

- ٨,٢,٢,٣,٢ على المرخص توظيف وبدوام كامل مختصي استجابة للحوادث السيبرانية من المواطنين السعوديين وذلك حسب ما يتم تحديده من قبل الهيئة.
- ٨,٢,٢,٣,٣ على المرخص تقديم الاستجابة والتحقيق في الحوادث السيبرانية من خلال كوادر سعودية مؤهلة وذوي خبرة من الحاصلين على شهادة تأهيل، حيث يجب أن تكون هذه الكوادر حاصلة على مؤهلات علمية وشهادات في مجال الأمن السيبراني أو المجالات ذات العلاقة، وأن تكون كوادر ذات خبرة في مجال الاستجابة والتحقيق في الحوادث السيبرانية، وذلك حسب ما يتم تحديده من قبل الهيئة.
- ٨,٢,٢,٣,٤ يجب على مقدمي خدمات الاستجابة لحوادث الأمن السيبراني الاحتفاظ بسجلات دقيقة وكاملة عن تفاصيل الحوادث السيبرانية التي يتم الاستجابة لها والتحقيق فيها لمدة (25) سنة من تاريخ تقديم تلك الخدمات، وتشمل تلك التفاصيل تاريخ تقديم الخدمة، واسم الجهة المستفيدة من الخدمة، وبيانات المستجيبين للحوادث الذين شاركوا في تقديم الخدمة، وأي طرف ثالث له علاقة في تقديم أي جزء من خدمات الاستجابة للحوادث السيبرانية. ويجب عدم إتلاف تلك المعلومات قبل تسليمها إلى الهيئة الوطنية للأمن السيبراني.
- ٨,٢,٢,٣,٥ يجب على مقدمي خدمات الاستجابة لحوادث الأمن السيبراني الاحتفاظ بنسخ دقيقة وكاملة للأدلة الرقمية المتعلقة بالحوادث السيبرانية التي يتم الاستجابة لها والتحقيق فيها لمدة لا تقل عن (١٠) سنوات من تاريخ تقديم تلك الخدمات؛ على أن تشمل - على سبيل المثال لا الحصر - سجلات الأنظمة والنسخ الرقمية للأقراص الصلبة والذاكرة العشوائية وغيرها. والتأكد من بقاء هذه النسخ دون تلف أو تغيير أو عبث أثناء جمعها وحفظها. ويجب عدم إتلاف تلك المعلومات قبل تسليمها إلى الهيئة الوطنية للأمن السيبراني.
- ٨,٢,٢,٣,٦ يجب على مقدمي خدمات الاستجابة لحوادث الأمن السيبراني القيام بالتحليل، وتقديم الإجراءات والتدابير، فيما يتعلق بعمليات الاستجابة للجهة المتأثرة من حادثة الأمن السيبراني. كما يتولى مقدمو خدمات الاستجابة لحوادث الأمن السيبراني مسؤولية المراجعة، وتقديم الدروس المستفادة للجهة المتأثرة من حادثة الأمن السيبراني بعد انتهاء الأعمال.
- ٨,٢,٢,٣,٧ يجب على مقدمي خدمات الاستجابة لحوادث الأمن السيبراني اتباع آلية ممنهجة لتقديم خدمات الاستجابة للحوادث على أن تتضمن الآلية صياغة تقرير نهائي شامل لتفاصيل الحادثة، وفق منهجية ونماذج تحددها الهيئة، وإرساله بالصيغة المطلوبة، وتحفظ الهيئة بحقها في تحديد آلية الاستجابة للحوادث السيبرانية، ومنهجيتها ومحتوياتها بالكامل، وكذلك بحقها في إدخال أي تعديلات أو حذف أي من عناصرها.
- ٨,٢,٢,٣,٨ على المرخص العمل وفق آلية تقديم خدمة الاستجابة والتحقيق في الحوادث السيبرانية في البند رقم ٧,٣.

## ٩. أحكام التراخيص في فئة الترخيص العام

### ٩,١ متطلبات الحصول على الترخيص في فئة الترخيص العام

يجب على الكيان الذي يرغب في الحصول على ترخيص من المستوى الأول أو الثاني لتقديم خدمات أو منتجات أو حلول الأمن السيبراني من فئة الترخيص العام الموضحة في القسم رقم (٦) من هذه الوثيقة، استيفاء متطلبات الحصول على الترخيص وتجديده، والمحافظة عليه، وفق الجدول الآتي:

| المتطلبات العامة                    |   |   |
|-------------------------------------|---|---|
| تصنيف المتطلبات                     | متطلبات المستوى الأول من فئة الترخيص العام (عام - ١)  | متطلبات المستوى الثاني من فئة الترخيص العام (عام - ٢)   |
| المتطلبات التنظيمية                 | <ul style="list-style-type: none"> <li>أن يكون الكيان يعمل بشكل نظامي في المملكة.</li> <li>تعبئة وتقديم نموذج طلب الترخيص.</li> <li>تزويد الهيئة ببيانات الكيان (السجل التجاري، وعقد التأسيس، ووثيقة العنوان الوطني، ونموذج تعيين ممثل رسمي للكيان موقع ومختوم ومصدق من الغرفة التجارية، ووثيقة تسجيل استثمار أجنبي من وزارة الاستثمار في حال وجود ملكية أجنبية للجهة).</li> <li>اجتياز الكيان لمتطلبات التأهيل اللازمة من منظومة حصين.</li> <li>وجود موقع إلكتروني مرتبط بالكيان يحتوي على فروع الكيان، خدمات أو حلول أو منتجات الأمن السيبراني التي يقدمها الكيان، وتقديم ما يثبت علاقة الموقع الإلكتروني بالكيان.</li> </ul> | <ul style="list-style-type: none"> <li>أن يكون الكيان يعمل بشكل نظامي في المملكة.</li> <li>تعبئة وتقديم نموذج طلب الترخيص.</li> <li>تزويد الهيئة ببيانات الكيان (السجل التجاري، وعقد التأسيس، ووثيقة العنوان الوطني، ونموذج تعيين ممثل رسمي للكيان موقع ومختوم ومصدق من الغرفة التجارية، ووثيقة تسجيل استثمار أجنبي من وزارة الاستثمار في حال وجود ملكية أجنبية للجهة).</li> <li>اجتياز الكيان لمتطلبات التأهيل اللازمة من منظومة حصين.</li> <li>وجود موقع إلكتروني مرتبط بالكيان يحتوي على فروع الكيان، خدمات أو حلول أو منتجات الأمن السيبراني التي يقدمها الكيان، وتقديم ما يثبت علاقة الموقع الإلكتروني بالكيان.</li> </ul> |
| المتطلبات المرتبطة بنشاط عمل الكيان | <ul style="list-style-type: none"> <li>أن يكون نشاط الأمن السيبراني أحد الأنشطة الرئيسية للكيان.</li> <li>يشترط ألا يقل رأس مال الكيان الراغب في الحصول على ترخيص في فئة الترخيص العام عن (٥٠٠,٠٠٠) خمسمائة ألف ريال.</li> </ul>  |   |

### ٩,٢ التزامات المرخص في فئة الترخيص العام

يجب على المرخص في كل الأحوال الالتزام بأحكام هذا الإطار، والقرارات، والتنظيميات، والأطر والضوابط، والتعليمات، والتوجيهات، والتعاميم، وما في حكمها؛ الصادرة عن الهيئة. كما يجب عليه الالتزام بما يلي:

- ٩,٢,١ الأنظمة واللوائح، والتنظيمات، والتعليمات، المعمول بها في المملكة العربية السعودية.
- ٩,٢,٢ البدء بتقديم الخدمات المرخص بها خلال (٣) أشهر من تاريخ إصدار الترخيص في الحد الأقصى؛ ما لم تقرر الهيئة خلاف ذلك.
- ٩,٢,٣ التقيّد بمتطلبات التوطين، وإبقاء جميع المعلومات والبيانات المرتبطة بتقديم الخدمات والمنتجات قبل أو أثناء أو بعد تقديمها لديه داخل المملكة العربية السعودية، وعدم تخزينها أو وضع نسخها منها خارج المملكة.
- ٩,٢,٤ تنفيذ ما تجري مشاركته من الهيئة من توصيات أو متطلبات سيبرانية وأمنية؛ بما في ذلك التنبيهات السيبرانية، وقواعد رصد التهديدات، ومؤشرات الاختراق. وتزويد الهيئة بالنتائج، وفق المتطلبات، والمدة المقررة منها.
- ٩,٢,٥ عدم نشر أي بيانات متعلقة بالأمن السيبراني، والمعلومات ذات الصلة، قبل الحصول على موافقة خطية من الهيئة.

- ٩,٢,٦ عدم نشر و/ أو مشاركة أي بيانات للجهات الوطنية (العامة أو الخاصة أو غيرها) التي يعمل معها المرخص سواء بشكل منفرد أو بعد تجميع تلك البيانات أو المعلومات، مع أي جهة؛ بأي مسوغ، ولأي مسوغ بما فيها الجهات الحكومية أو الخاصة، داخل المملكة وخارجها؛ ويكون نشرها مشروطاً بموافقة خطية من الهيئة.
- ٩,٢,٧ النص في تعاقده، ذات الصلة بهذا الإطار على الأحكام التي تعالج حالات انتهاء الترخيص، أو عدم تجديده، أو إلغائه.
- ٩,٢,٨ إبلاغ الهيئة فوراً بأي تغيير في المعلومات، أو البيانات ذات الصلة بطلب الترخيص و/ أو المرخص، و/ أو عند اكتشاف أي معلومات غير دقيقة أو مخالفة للواقع، لما جرى إبلاغ الهيئة بها، مع بيان الأسباب التي دعت لتقديمها بشكل غير دقيق، أو غير صحيح، وسبب التغيير فيها.
- ٩,٢,٩ إبلاغ الهيئة فوراً بأي إجراء قانوني أو تنظيمي ضده قد يؤثر على تقديم الخدمات؛ بغض النظر عن الجهة التنظيمية أو الاختصاص، وسواء أكان من داخل المملكة أم كان خارجها.
- ٩,٢,١٠ التعاون التام مع الهيئة عند مباشرة اختصاصاتها التنظيمية والرقابية عليه بوصفه مرخص له، وإتاحة جميع الموارد الممكنة الخاصة به، لتنفيذ أي متطلبات للرقابة، والتفتيش من الهيئة، بما يشمل المراجعة والتحقق، وإجراء التقييمات السيبرانية، وأي متطلب آخر على أعماله وأنظمتها أي كانت.
- ٩,٢,١١ الالتزام بالقرارات الصادرة عن الهيئة، في أي خلافات قد تنشأ مع الجهة المتعاقد معها.
- ٩,٢,١٢ الالتزام بنسب المحتوى المحلي على مستوى الكيان، والتوطين للوظائف من الكفاءات الوطنية؛ وفق ما تقره الهيئة، والجهات المختصة.
- ٩,٢,١٣ الالتزام بالمسؤوليات والواجبات عند تقديم خدمات وحلول ومنتجات الأمن السيبراني للجهات الوطنية، وفق ما يصدر من الهيئة.
- ٩,٢,١٤ التطبيق الكامل والمستمر لجميع ضوابط الأمن السيبراني، الصادرة عن الهيئة، التي تنطبق على المرخص؛ وتشمل -دون حصر- الضوابط الأساسية للأمن السيبراني، وضوابط الأمن السيبراني للأنظمة الحساسة، وضوابط الأمن السيبراني للبيانات، وتقديم وثائق سنوية تثبت الالتزام بالضوابط المعتمدة من قبل الهيئة.
- ٩,٢,١٥ الالتزام بإشعار الهيئة فوراً عندما يطرأ أي تغيير في ملكية كيان المرخص، بأي شكل كان.
- ٩,٢,١٦ الالتزام بالحصول على موافقة الهيئة، الخطية المسبقة؛ قبل ترتيب أي إجراء من شأنه تحقيق تغيير في ملكية كيان المرخص، بأي شكل كان.
- ٩,٢,١٧ الالتزام بالقرارات والتعليمات الصادرة عن الهيئة، بما في ذلك تلك المتعلقة بأي خلافات قد تنشأ مع الجهة المتعاقد معها، تجاه الخدمات أو الحلول أو المنتجات المقدمة بموجب الترخيص.
- ٩,٢,١٨ تزويد الهيئة بالتقارير الدورية -وفق ما تقره- وأي معلومات أخرى تطلبها، والتقيّد بالمدد الزمنية ذات الصلة، والكيفية والنماذج المقررة لذلك، وتشمل التقارير -على سبيل المثال لا الحصر- الخدمات والمنتجات والحلول التي تم تقديمها للجهات الوطنية المستفيدة، وغيرها.
- ٩,٢,١٩ على المرخص لتقديم خدمات ومنتجات وحلول الأمن السيبراني الاحتفاظ بسجلات دقيقة وكاملة عن خدمات ومنتجات وحلول الأمن السيبراني المقدمة للجهات الوطنية المستفيدة، لمدة (٥) سنوات من تاريخ تقديم تلك الخدمات والمنتجات والحلول؛ على أن تشمل -على سبيل المثال لا الحصر- تاريخ تقديم الخدمات والمنتجات والحلول، واسم الجهة المستفيدة من الخدمات والمنتجات والحلول، وأي طرف ثالث له علاقة في تقديم أي جزء من خدمات ومنتجات وحلول الأمن السيبراني.
- ٩,٢,٢٠ على المرخص الذي يعمل ضمن المجالات الفرعية المتعلقة بتقديم منتجات وحلول الأمن السيبراني الالتزام بالآتي:
- ٩,٢,٢٠,١ تزويد الهيئة بتفاصيل المنتج أو الحل والمستخدمين في المملكة بصفة دورية.
- ٩,٢,٢٠,٢ إبلاغ الهيئة الوطنية للأمن السيبراني بشكل فوري عن أي ثغرات أو مخاطر سيبرانية حرجة أو حالات تسريب للبيانات يتم اكتشافها أو تلقي إشعار بوجودها في المنتجات أو الحلول التي يتم تقديمها أو توفيرها من قبلهم، وتقديم خطة معالجة أولية للهيئة خلال فترة وجيزة، وذلك من خلال منصة (حصين).

- ٩,٢,٢٠,٣ توفير فريق للتواصل مع الهيئة على مدار الساعة (٧/٢٤) بشأن أي حالات ترتبط بمخاطر وتهديدات قد تطرأ على المنتج أو الحل.
- ٩,٢,٢٠,٤ إجراء التقييمات السيبرانية اللازمة لضمان أمن منتجات أو حلول الأمن سيبراني المقدمة من قبل المرخص، وفق ما يصدر من الهيئة.
- ٩,٢,٢٠,٥ تفعيل آليات التشفير وحماية البيانات عند نقلها عبر الشبكات باستخدام خوارزميات معتمدة دولياً، أو خوارزميات التشفير وفق ما يصدر من الهيئة.
- ٩,٢,٢٠,٦ اتباع منهجية معتمدة للتطوير الآمن للبرمجيات.
- ٩,٢,٢٠,٧ الالتزام بكافة المعايير أو الضوابط للفسح والترخيص باستيراد وتصدير واستخدام الأجهزة والبرمجيات ذات الحساسية العالية للأمن السيبراني التي تحددها الهيئة.

## ١.٠ طلب الحصول على الترخيص والمحافظة عليه وتجديده

- ١٠,١ يجب للحصول على ترخيص تقديم الخدمات ضمن فئة الترخيص المتخصص؛ التقدّم بطلب للهيئة، واستيفاء المتطلبات المنصوص عليها في المتطلبات الواردة في البند رقم (٨,١) حسب الخدمة المراد الحصول على الترخيص لها ومستواها، وكذلك المتطلبات الواردة في الملحق (ب) من هذا الإطار.
- ١٠,٢ يجب للحصول على ترخيص تقديم الخدمات أو المنتجات أو الحلول ضمن فئة الترخيص العام؛ التقدّم بطلب للهيئة، واستيفاء المتطلبات المنصوص عليها في المتطلبات الواردة في البند رقم (٩,١)، وكذلك المتطلبات الواردة في الملحق (ب) من هذا الإطار.
- ١٠,٣ تكون مدة ترخيص تقديم الخدمات أو المنتجات أو الحلول (٥) خمس سنوات تبدأ من تاريخ إصداره.
- ١٠,٤ يجب على المرخص الاستمرار بالوفاء بالمتطلبات والالتزامات المنصوص عليها في البند رقم (٨,١) والبند رقم (٨,٢) من هذه الوثيقة والملحق (ب) للمحافظة على الترخيص، الصادر له بحسب مستواه ونوع الخدمة من فئة الترخيص المتخصص.
- ١٠,٥ يجب على المرخص الاستمرار بالوفاء بالمتطلبات والالتزامات المنصوص عليها في البند رقم (٩,١) والبند رقم (٩,٢) من هذه الوثيقة والملحق (ب) للمحافظة على الترخيص من فئة الترخيص العام.
- ١٠,٦ يجوز للمرخص التقدّم بطلب لتجديد الترخيص، في موعد لا يتجاوز (٩٠) يوم تقويمي قبل تاريخ انتهاء الترخيص، وفي موعد أقصاه (٣٠) يوم تقويمي قبل تاريخ انتهاء الترخيص، واستيفاء جميع المتطلبات التنظيمية ذات العلاقة المنصوص عليها في هذا الإطار وأي متطلبات أخرى تفرضها الهيئة.
- ١٠,٧ في حال عدم رغبة المرخص في تجديد الترخيص، أو في حال رفض الهيئة لطلب التجديد الذي تقدّم به، أو في حال كون المرخص قد قام بتقديم طلب لإلغاء الترخيص (في أي من هذه الحالات)، فيتوجب عليه عدم استقبال أي تعاقدات جديدة داخلية في نطاق الترخيص، وأن يُشعر الجهات المتعاقد معها، وفق ما تقرره الهيئة.

## ١.١ التنازل عن الترخيص

- ١١,١ لا يجوز للمرخص التنازل عن الترخيص الصادر له، دون الحصول على موافقة خطية مسبقة من الهيئة.
- ١١,٢ يجب على المرخص الذي يرغب في التنازل عن الترخيص الصادر له؛ التقدّم بطلب خطي إلى الهيئة يتضمّن الأسباب والحيشيات لطلب التنازل؛ وتقديم أي معلومات أو وثائق إضافية تطلبها الهيئة، أثناء دراسة الطلب.
- ١١,٣ تصدر الهيئة قرارها في شأن الطلب ويتوجب على المرخص التقيّد به.

## ١٢. إلغاء الترخيص وتعليقه

- ١٢,١ يجب على المرخص الذي يرغب في إلغاء الترخيص الصادر له؛ التقدّم بطلب خطي إلى الهيئة، يتضمّن الأسباب والحيثيات لطلب الإلغاء؛ وكذلك تقديم أي معلومات أو وثائق إضافية تطلبها الهيئة أثناء دراسة الطلب. وتصدر الهيئة -بعد تلقي طلب الإلغاء المكتمل من المرخص- قرارها في شأن الطلب؛ ويتوجّب على المرخص التقيد به.
- ١٢,٢ تحتفظ الهيئة -وفقاً لتقديرها- بحق إلغاء الترخيص أو تعليقه؛ في الحالات التي تستلزم ذلك، ومن تلك الحالات -على سبيل المثال لا الحصر:-
- أ. عدم الالتزام بالأحكام المنصوص عليها في هذا الإطار، وما يطرأ عليه من تعديلات.
- ب. عدم الالتزام بأي وثائق أو متطلبات تنظيمية صادرة عن الهيئة، ويشمل ذلك القرارات، والتنظيمات، والأطر والتعليمات، والتوجيهات، والتعاميم، والضوابط وما في حكمها.
- ج. تكرار حالات عدم الوفاء بالالتزامات المقررة على المرخص بموجب هذا الإطار، وتنظيمات الهيئة ذات العلاقة.
- ١٢,٣ يحتسب تعليق الترخيص ضمن مدة سريان الترخيص، ولا يكون له تأثير في تاريخ انتهاء الترخيص.
- ١٢,٤ ستقوم الهيئة برفع تعليق الترخيص؛ وفقاً لتقديرها المطلق، وبعد اتخاذ المرخص الإجراءات التصحيحية اللازمة، المفروضة عليه من الهيئة، وقبولها منه.
- ١٢,٥ لا يُسمح للمرخص، بأي شكل كان؛ تقديم خدماته الداخلة، في نطاق الترخيص، عند انتهاء الترخيص الصادر له، أو إلغائه أو تعليقه.

## ١٣. التعاقد من الباطن

- ١٣,١ لا يجوز للمرخص؛ التعاقد من الباطن، إلا من خلال مرخصين آخرين ضمن نفس الفئة والمستوى التي يحملون ترخيصاً لها. وعلى هذا؛ فإنه لا يجوز للمرخصين من المستوى الأول من فئة الترخيص المتخصص (متخصص - ١) التعاقد من الباطن؛ إلا من خلال مقدمي خدمات مرخصين من المستوى الأول من فئة الترخيص المتخصص (متخصص - ١). وينطبق الأمر نفسه على جميع أنواع التراخيص. لايجوز للمرخص التعاقد من الباطن لتقديم خدمات أو منتجات أو حلول الأمن السيبراني إلا من خلال مرخص آخر لنفس الخدمة أو المنتج أو الحل.
- ١٣,٢ يجوز للمرخص التعاقد من الباطن؛ لتقديم خدمات أو منتجات أو حلول الأمن السيبراني، وفقاً للشروط الآتية:
- ١٣,٢,١ إشعار الهيئة بذلك، وفق المتطلبات التي تقررها الهيئة.
- ١٣,٢,٢ عدم السماح مباشرة الجهة المتعاقد معها من الباطن لأي أعمال، قبل الحصول على موافقة الهيئة بالتعاقد من الباطن.
- ١٣,٢,٣ تظل جميع الالتزامات الناشئة عن الترخيص في مواجهة الهيئة، مسؤولية المرخص، وتكون أي اشتراطات، أو قيود تخالف ذلك في التعاقدات، بين المرخص، والمرخص المتعاقد معه من الباطن؛ باطلة، ولا ترتّب أي أثر قانوني لها تجاه الهيئة.
- ١٣,٢,٤ يجب توثيق ترتيبات التعاقد من الباطن، ضمن هذا البند؛ في سجلات المرخص الداخلية، والتقيد بأي تعليمات للهيئة ذات صلة.
- ١٣,٣ للهيئة وفق تقديرها المطلق؛ وضع حد أعلى للتعاقدات من الباطن، التي يجوز للمرخص في المستوى الأول القيام بها.
- ١٣,٤ في كل الأحوال يجب أن يفي المتعاقد معه من الباطن، بجميع الالتزامات المقررة على المرخص بموجب هذا الإطار.

## ١٤. أحكام عامة

- ١٤,١ يجب على أي كيان، يقدم خدمات أو منتجات أو حلول أمن سيبراني في المملكة، أو يرغب في تقديمها؛ الحصول على ترخيص بذلك من الهيئة، وفقاً للأحكام الواردة في هذا الإطار؛ وما تقره الهيئة.
- ١٤,٢ ستقرر الهيئة مهلة تصحيحية للكيانات العاملة في تقديم خدمات ومنتجات وحلول الأمن السيبراني، التي تدخل في نطاق هذا الإطار. ويجب على تلك الكيانات معالجة أوضاعها، بما يتفق مع هذا الإطار، وما يصدر عن الهيئة.
- ١٤,٣ ستصدر الهيئة التعليمات والضوابط ذات الصلة، التي يجب على الكيانات التي تدخل في نطاق هذا الإطار؛ التقيّد بها في التعاقدات القائمة، أو المستقبلية لهم.
- ١٤,٤ يجب على جميع الكيانات التي تدخل في نطاق هذا الإطار؛ تقديم جميع الوثائق والمعلومات والتعاقدات، ذات الصلة بهذه الخدمات، وأي معلومات أخرى للهيئة، وفق ما تقره، وذلك خلال مدة لا تتجاوز (٣٠) يوماً من تاريخ نفاذ هذا الإطار.
- ١٤,٥ للهيئة وفق ما تقتضيه متطلبات تنظيم القطاع؛ فرض قيود أو متطلبات إضافية، أو إلغاؤها على المرخص، أو الفرد الحاصل على شهادة التأهيل.
- ١٤,٦ تحتفظ الهيئة بحقها في رفض أي طلبات للحصول على الترخيص، أو تجديده، أو إلغائه بموجب هذا الإطار.
- ١٤,٧ يلتزم كل من المرخص، بتقديم التقارير الدورية إلى الهيئة، وأي معلومات أخرى تطلبها وفق ما تقره.
- ١٤,٨ مع مراعاة الأحكام الواردة في هذا الإطار، بشأن إلغاء الترخيص أو تعليقه، سوف تتخذ الهيئة القرارات اللازمة تجاه أي مخالفة مرتكبة، بموجب هذا الإطار، وفقاً لصلاحياتها النظامية.
- ١٤,٩ تحتفظ الهيئة بحقها في فرض مقابلات مالية أخرى على المرخص.
- ١٤,١٠ تعد الملاحق الواردة في هذا الإطار جزءاً منه، ويتم قراءتها والعمل بها كوثيقة واحدة.
- ١٤,١١ تعد النسخة العربية من هذا الإطار؛ هي النسخة الرسمية المعتمدة، وفي حال وجود أي اختلافات بين نص النسخة الرسمية المكتوبة باللغة العربية، والترجمة إلى اللغات الأخرى؛ فيتم الرجوع إلى النسخة العربية.
- ١٤,١٢ يجوز للهيئة مراجعة هذا الإطار وتحديثه، وفق متطلبات تنظيم قطاع الأمن السيبراني ويجب التقيّد بما يطرأ عليه من تحديث، وفق ما تقره الهيئة.
- ١٤,١٣ يحق للهيئة عدم منح الترخيص أو إلغاؤه أو تعليقه وذلك لحماية الأمن الوطني، على أن يكون قرارها مبنياً على أساس موضوعي وبالتنسيق مع الجهات المختصة.

## ١٥. الملحق

### الملحق (أ): خدمات ومنتجات وحلول الأمن السيبراني

| ١ منتجات وحلول الأمن السيبراني             |   |
|--|---|
| ١-١ أمن الأجهزة الطرفية وإدارتها           |   |
| فئة الترخيص لتقديم الخدمة / المنتج أو الحل | حلول الأمن السيبراني لحماية الأجهزة الطرفية، بما يشمل الخوادم والأجهزة المكتبية والأجهزة المحمولة.  |
| فئة الترخيص العام                          | ١-١-١ حلول أمن المتصفح<br>حلول أمن الأجهزة الطرفية لتأمين متصفحات الويب، والمتصفحات المحلية الآمنة، ووظائف المتصفحات الإضافية.  |
| فئة الترخيص العام                          | ٢-١-١ حلول أمن الأجهزة الطرفية<br>حلول أمن الأجهزة الطرفية لتأمين الأجهزة الشخصية والخوادم وغيرها، من خلال الكشف عن البرامج الضارة والفيروسات وبرمجيات حصان طروادة وبرمجيات الابتزاز وما إلى ذلك والوقاية منها. |
| فئة الترخيص العام                          | ٣-١-١ حلول الرصد والاستجابة لدى الأجهزة الطرفية (EDR)<br>حلول أمن الأجهزة الطرفية لإجراء تحليلات مباشرة للتهديدات والاحتواء والتحقيق والاستجابة.  |
| فئة الترخيص العام                          | ٤-١-١ حلول حماية الأجهزة المحمولة<br>حلول أمن الأجهزة الطرفية والتطبيقات التي تحمي الأجهزة المحمولة وتطبيقاتها/بياناتها.  |
| فئة الترخيص العام                          | ٥-١-١ حلول إدارة الأجهزة المحمولة (MDM)<br>حلول أمن الأجهزة الطرفية لإدارة وتطبيق السياسات المرتبطة بالأجهزة المملوكة للجهات وأجهزة الموظفين.   |
| فئة الترخيص العام                          | ٦-١-١ حلول جدار الحماية للأجهزة<br>حلول أمن الأجهزة الطرفية التي تنشئ برمجيات جدار الحماية لحماية الأجهزة الطرفية من الاتصالات الخبيثة.   |
| فئة الترخيص العام                          | ٧-١-١ حلول إدارة الإعدادات الأمنية<br>حلول أمن الأجهزة الطرفية لإدارة الإعدادات الأمنية للأجهزة الطرفية للجهات ومراقبتها.   |
| فئة الترخيص العام                          | ٨-١-١ حلول إدارة الأصول<br>حلول أمن الأجهزة الطرفية المستخدمة في إدارة كافة الأصول على مستوى الجهة، بما يشمل اكتشاف الأصول وقاعدة بيانات إعدادات الأصول.  |

|  |  |  |       |
|--|--|--|-------|
| فئة الترخيص العام                          | حلول أمن الأجهزة الطرفية لتحديد الإصلاحات وترتيبها حسب الأولوية واختبارها وتطبيقها على مستوى الجهة.  | حلول إدارة وإعداد حزم التحديثات والإصلاحات         | ٩-١-١ |
| أمن الشبكات                                |  |  | ٢-١   |
| فئة الترخيص لتقديم الخدمة / المنتج أو الحل | حلول الأمن السيبراني لحماية البنية التحتية من الشبكات بدءًا من محيط الشبكة إلى الأجهزة الطرفية.  |  |       |
| فئة الترخيص العام                          | حلول أمن الشبكات التي تفحص الحركة في الشبكة وتكشف المحتوى الضار وترسل التنبيهات (للكشف فقط) واتخاذ الإجراءات مثل الحظر (الكشف والوقاية).   | أنظمة اكتشاف ومنع التسلل (IDPS)                    | ١-٢-١ |
| فئة الترخيص العام                          | حلول أمن الشبكات التي تتيح للجهات الوصول إلى شبكات الجهة عن طريق المصادقة والإعدادات وإذن الدخول حسب الدور والسياسات الأخرى.   | حلول التحكم بدخول الشبكات                          | ٢-٢-١ |
| فئة الترخيص العام                          | حلول أمن الشبكات التي تستخدم القواعد لمراقبة الحركة الصادرة والواردة الضارة في الشبكة وحضرها، بما يشمل الجيل القادم من جدار الحماية التي تتمتع بخصائص متقدمة مثل الفحص العميق للحزم. | حلول جدار حماية الشبكات                            | ٣-٢-١ |
| فئة الترخيص العام                          | حلول أمن الشبكات التي تعمل على تصفية حركة المستخدمين وتحظر المحتوى الضار أو غير المرغوب (مثل: المحتويات ضد سياسات الجهة).  | حلول بوابة الويب الآمنة (SWG)                      | ٤-٢-١ |
| فئة الترخيص العام                          | حلول أمن الشبكات، المؤتمتة واليدوية، التي تسمح بتحليل المحتوى المرعب في بيئة معزولة.   | حلول العزل والحماية من التهديدات المتقدمة المستمرة | ٥-٢-١ |
| فئة الترخيص العام                          | حلول أمن الشبكات التي تكون بمثابة وسيط بين المستخدم وشبكة الإنترنت، بما يزيد الكفاءة والأمن والخصوصية.   | حلول الخوادم الوكيل (Proxy)                        | ٦-٢-١ |
| فئة الترخيص العام                          | حلول أمن الشبكات التي تُطرح بمثابة فخ لخداع المهاجمين للابتعاد عن الأصول القيّمة وإعطاء فرق الأمن الفرصة للتحقيق في الهجمات والتعامل معها.   | حلول مصائد الهجمات (Honeynets/Honeypots)           | ٧-٢-١ |
| فئة الترخيص العام                          | حلول أمن الشبكات للمؤسسات الصغيرة والمتوسطة التي تضم عدة أقسام وظيفية، مثل جدار الحماية وتصفية المحتوى ومضاد الفيروسات وغير ذلك.   | الحلول الموحدة لإدارة التهديدات (UTM)              | ٨-٢-١ |

|  |   |  |       |
|--|---|--|-------|
| فئة الترخيص العام                          | حلول أمن الشبكات للكشف عن الهجمات الموزعة لحجب الخدمة التي تحاول إغراق شبكة الجهة والحد من توافرها لتلبية الطلبات الحقيقية، والحماية منها.  | حلول الحماية من هجمات حجب الخدمة الموزعة (DDoS)        | ٩-٢-١ |
|  |   | أمن البيانات   | ٣-١   |
| فئة الترخيص لتقديم الخدمة / المنتج أو الحل | حلول الأمن السيبراني التي تتيح حماية البيانات والتي تغطي البيانات الثابتة والمتنقلة.  |  |       |
| فئة الترخيص العام                          | حلول أمن البيانات التي تحدد البيانات الحساسة وتصنيفها حسب التصنيف الملائم.  | حلول اكتشاف البيانات وتصنيفها                          | ١-٣-١ |
| فئة الترخيص العام                          | حلول أمن البيانات المتاحة للأجهزة الطرفية والشبكات لمنع فقادات البيانات الحساسة أو تسريبها.   | حلول منع فقدان البيانات (DLP)                          | ٢-٣-١ |
| فئة الترخيص العام                          | حلول أمن البيانات التي تُسهّل حماية المعلومات الحساسة ضمن البيانات، إما باستبدالها برمز (الترميز) أو حجب أو إزالة البيانات الحساسة (الحجب).   | حلول إخفاء البيانات وترميزها                           | ٣-٣-١ |
| فئة الترخيص العام                          | حلول أمن البيانات التي تحمي البيانات الثابتة (مثل الملفات والمجلدات وغير ذلك) باستخدام التشفير لمنع الوصول غير المصرح به، وتتضمن أيضاً الأنظمة التي تدير مفاتيح التشفير (مثل الإنشاء والتوزيع والإتلاف وغيرها). | حلول تشفير الأجهزة الطرفية وأنظمة إدارة المفاتيح (KMS) | ٤-٣-١ |
| فئة الترخيص العام                          | حلول أمن البيانات التي تحمي البيانات المتنقلة، وتؤمن البروتوكولات الآمنة (SSL/TLS).   | حلول تشفير الشبكات                                     | ٥-٣-١ |
| فئة الترخيص العام                          | حلول أمن البيانات التي تحمي قواعد البيانات وحاويات التخزين الأخرى، بما يشمل المراقبة والتحكم في الوصول والتشفير والتدقيق وغير ذلك؟  | حلول أمن قواعد البيانات والتخزين                       | ٦-٣-١ |
| فئة الترخيص العام                          | حلول أمن البيانات لمشاركة البيانات بشكل آمن.  | حلول النقل الآمن للملفات                               | ٧-٣-١ |
| فئة الترخيص العام                          | حلول أمن البيانات التي تفحص البريد الإلكتروني الوارد العشوائي والضرر وتحجبه (للحماية من التهديدات المستمرة المتقدمة للبريد الإلكتروني).   | بوابة البريد الإلكتروني الآمنة (SEG)                   | ٨-٣-١ |
| فئة الترخيص العام                          | حلول أمن البيانات لإدارة البيانات الشخصية وحمايتها على مدار دورة حياتها بما يشمل الالتزام والقبول والتحكم والتدقيق في ذلك.  | حلول تقنيات تعزيز الخصوصية (PET)                       | ٩-٣-١ |

|  |  |   |                   |
|--|--|---|-------------------|
| ١٠-٣-١   | حلول إدارة الحقوق الرقمية (DRM)              | حلول أمن البيانات المستخدمة في تقييد الوصول إلى المحتوى المحمي وإدارته.   | فئة الترخيص العام |
| ١١-٣-١   | حلول الحماية من برمجيات الفدية               | حلول أمن البيانات المصممة خصيصًا لمنع تهديدات برمجيات الابتزاز والكشف عنها والاستجابة لها.  | فئة الترخيص العام |
| ٤-١  | أمن التطبيقات                                |   |                   |
| حلول الأمن السيبراني التي تتيح الحماية على مستوى التطبيقات.  |  |   |                   |
| ١-٤-١  | حلول اختبار أمن التطبيقات (AST)              | حلول أمن التطبيقات لتحليل التطبيقات واختبارها لتحديد الثغرات الأمنية بما يشمل اختبار أمن التطبيقات الثابتة (SAST)، واختبار أمن التطبيقات الديناميكية (DAST)، واختبار أمن التطبيقات التفاعلية (IAST)، وكشف الهجمات في الوقت الفعلي للتطبيقات (RASP). | فئة الترخيص العام |
| ٢-٤-١  | حلول جدار حماية تطبيقات الويب (WAF)          | حلول أمن التطبيقات التي تحمي تطبيقات الويب بفرز طلبات HTTP/S ومراقبتها للكشف عن الأنشطة الضارة.   | فئة الترخيص العام |
| ٣-٤-١  | حلول التحكم في التطبيقات                     | حلول أمن التطبيقات لتحديد قائمة التطبيقات المعتمدة لاستخدامها في المنظمة وتقييد تنفيذ التطبيقات غير المعتمدة (بما يشمل القائمة البيضاء والقائمة السوداء للتطبيقات).   | فئة الترخيص العام |
| ٤-٤-١  | حلول أمن واجهة برمجة تطبيقات الويب (Web API) | حلول أمن التطبيقات لحماية واجهات برمجة تطبيقات الويب (Web API). بهدف تأمين نقل البيانات عن طريق واجهات برمجة التطبيقات ومنع الهجمات الضارة على واجهات تطبيقات الويب أو إساءة استخدامها.   | فئة الترخيص العام |
| ٥-١  | إدارة هويات الدخول والصلاحيات                |   |                   |
| حلول الأمن السيبراني التي تتيح حوكمة وإدارة الهويات الرقمية للتطبيقات ضمن بيئة تقنية المعلومات والتقنية التشغيلية. |  |   |                   |
| فئة الترخيص لتقديم الخدمة / المنتج أو الحل   |  |   |                   |

|  |   |  |       |
|--|---|--|-------|
| فئة الترخيص العام                          | حلول أمن الهوية وإدارتها المستخدمة في تخزين بيانات اعتماد المستخدمين وإدارتها بشكل آمن.   | حلول إدارة كلمات المرور                | ١-٥-١ |
| فئة الترخيص العام                          | حلول أمن الهوية وإدارتها لإدارة هويات المستخدمين على مستوى المنظمة أو المنظومة، بما يشمل الهوية الرقمية الموحدة.  | حلول حوكمة الهويات                     | ٢-٥-١ |
| فئة الترخيص العام                          | حلول أمن الهوية وإدارتها والتي تتيح التحكم بالوصول عن طريق المصادقة المركزية وتسجيل الدخول لمرة واحدة (SSO) والدخول عن بعد وإدارة الجلسات وغير ذلك.     | حلول إدارة صلاحيات الدخول              | ٣-٥-١ |
| فئة الترخيص العام                          | حلول أمن الهوية وإدارتها لتأمين الوصول المتقدم إلى الأصول الحساسة وإدارتها.   | حلول إدارة صلاحيات الدخول المميز (PAM) | ٤-٥-١ |
| فئة الترخيص العام                          | حلول أمن الهوية وإدارتها والتي تتحقق من الهوية الرقمية للأفراد وتتيح الوصول إلى الحلول.   | حلول التحقق                            | ٥-٥-١ |
| فئة الترخيص العام                          | حلول أمن الهوية وإدارتها لتخزين الشهادات الرقمية التي تصدق هويات الأطراف الموثوقة، وتوقيعها وإصدارها.   | حلول إدارة الشهادات الرقمية            | ٦-٥-١ |
| فئة الترخيص العام                          | حلول أمن الهوية وإدارتها التي تمكن مستويات أعلى من الثقة، مثل: الحوسبة الموثوقة (TC)، الأمن المتعدد المجالات (CDS)، والحلول الأمنية المتعددة المستويات. | حلول الحوسبة عالية الثقة               | ٧-٥-١ |
| فئة الترخيص العام                          | حلول أمن الهوية وإدارتها والتي تتيح عناصر مصادقة إضافية مثل الرموز المشفرة والخصائص الحيوية وغير ذلك.   | حلول التحقق متعدد العناصر              | ٨-٥-١ |
| الحوكمة والمخاطر والالتزام                 |   |  | ٦-١   |
| فئة الترخيص لتقديم الخدمة / المنتج أو الحل | حلول الأمن السيبراني التي تتيح تخطيط الحوكمة وإدارة المخاطر وإدارة الالتزام لبيئة تقنية المعلومات والتقنية التشغيلية                                    |  |       |

|  |  |   |
|--|--|---|
| ١-٦-١                                      | حلول الحوكمة والمخاطر والالتزام لمتابعة المخاطر السيبرانية للمؤسسة وبرامج الالتزام ومسؤولياته، وإدارتها.   | حلول الحوكمة والمخاطر والالتزام (GRC)       |
| ٢-٦-١                                      | حلول الحوكمة والمخاطر والالتزام التي تحمي ضد مخاطر سلسلة الإمداد، بما يشمل تقييم مخاطر الموردين وحلول أمن إدارة الموردين.  | حلول إدارة مخاطر الأطراف الخارجية (TPRM)    |
| ٧-١  | حلول عمليات الأمن السيبراني  |   |
| فئة الترخيص لتقديم الخدمة / المنتج أو الحل | حلول الأمن السيبراني المستخدمة لتنفيذ أنشطة ومهام الأمن السيبراني اليومية.   |   |
| ١-٧-١                                      | حلول أمنية متكاملة تُعنى بتوسيع نطاق عمليات الكشف عن التهديدات والاستجابة لها عبر بيئات متعددة (مثل: الشبكات، الأجهزة الطرفية، الخوادم، التطبيقات، السحابة، البريد الإلكتروني، الهوية)، وذلك من خلال دمج وتحليل البيانات الأمنية من مصادر متنوعة في منصة موحدة. تهدف إلى الوصول لرؤية شاملة، تحليل التهديدات المعقدة، وأتمتة الاستجابة بشكل استباقي. | حلول الكشف والاستجابة الممتدة (XDR)         |
| ٢-٧-١                                      | حلول عمليات الأمن السيبراني باستخدام التحليلات الأمنية للكشف عن أي تهديدات للشبكة من جهات معروفة أو غير معروفة وتقليل مخاطرها.   | حلول الاكتشاف والاستجابة للشبكات (NDR)      |
| ٣-٧-١                                      | حلول عمليات الأمن السيبراني التي تدعم الكشف الاستباقي للتهديدات النشطة والجهات التخريبية غير المعروفة مسبقاً.  | حلول تصيد التهديدات السيبرانية              |
| ٤-٧-١                                      | حلول عمليات الأمن السيبراني لتحديد الأدلة الإلكترونية والحصول عليها وتحليلها واستكمال التحقيقات بالاستعانة بالحاسوب.   | حلول التحقيق الجنائي الرقمي                 |
| ٥-٧-١                                      | حلول عمليات الأمن السيبراني المستخدمة في الكشف عن الإجراءات المرعبة استناداً إلى السلوكيات المعيارية، بما يشمل الكشف عن الاحتيال والوقاية منه.   | حلول تحليل السلوكيات واكتشاف الحالات الشاذة |
| ٦-٧-١                                      | حلول عمليات الأمن السيبراني التي من شأنها تحديد الثغرات الأمنية وتصنيفها وإدارتها.   | حلول المسح وتقييم الثغرات                   |

|   |   |   |                   |
|---|---|---|-------------------|
| 7-7-1   | حلول اختبار الاختراقات  | حلول عمليات الأمن السيبراني للكشف عن نقاط الضعف التي يمكن استغلالها في الوضع الأمني، واختبارها وتصنيفها، مثل: رفع الامتيازات.   | فئة الترخيص العام |
| 8-7-1   | حلول إدارة الحوادث والتنسيق الأمني والأتمتة والاستجابة (SOAR) | حلول عمليات الأمن السيبراني التي من شأنها تنسيق الاستجابة إلى الأحداث الأمنية وأتمتتها وإدارتها.  | فئة الترخيص العام |
| 9-7-1   | حلول إدارة المعلومات والأحداث الأمنية (SIEM)                  | حلول عمليات الأمن السيبراني لجمع الأحداث وإدارة السجلات وتصحيح السجلات.   | فئة الترخيص العام |
| 10-7-1  | حلول المعلومات الاستباقية عن التهديدات السيبرانية             | حلول عمليات الأمن السيبراني لاستيعاب النوايا والأهداف وتقنيات الهجوم للجهات التخريبية، وتحليلها وفحصها، بما يشمل الاستخبارات القابلة للقراءة آلياً مثل مؤشرات الاختراق (IoC). | فئة الترخيص العام |
| 11-7-1  | أدوات التوعية والتدريب في مجال الأمن السيبراني                | حلول عمليات الأمن السيبراني لصقل مهارات المستخدمين ومختصي الأمن السيبراني، مثل الحملات المضادة للتصيد الاحتيالي والنطاقات السيبرانية وغير ذلك.                                | فئة الترخيص العام |
| 8-1   | أمن الحوسبة السحابية  |   |                   |
| حلول الأمن السيبراني التي تتيح حماية التطبيقات القائمة على الحوسبة السحابية.    |   |   |                   |
| 1-8-1   | حلول وسطاء الأمان للوصول إلى السحابة (CASB)                   | حلول أمن الحوسبة السحابية لإضافة الضوابط الأمنية إلى خدمات الحوسبة السحابية وضمان التزام المستخدمين بسياسات استخدام الحوسبة السحابية.   | فئة الترخيص العام |
| 2-8-1   | أمن الجهد السحابي   | حلول أمن الحوسبة السحابية، التي تحمي الجهد أثناء التنقل بين بيئات الحوسبة السحابية المختلفة.  | فئة الترخيص العام |
| 9-1   | أمن الأنظمة الخاصة  |   |                   |
| حلول الأمن السيبراني التي تتيح حماية الأنظمة الخاصة مثل التقنية التشغيلية (OT). |   |   |                   |
| 1-9-1   | حلول الأمن الصناعي  | حلول أمن الأنظمة الخاصة لحماية أنظمة التحكم الصناعية (ICS)، والتقنية التشغيلية (OT) بما يشمل واجهة المستخدم والآلة (HMI)، والتحكم الإشرافي                                    | فئة الترخيص العام |

|  |   |   |       |
|--|---|---|-------|
|  | وتحصيل البيانات (SCADA)، والبيانات والأمن السيبراني لأنظمة التحكم الموزعة (DSC).  |   |       |
| فئة الترخيص العام                          | حلول أمن الأنظمة الخاصة التي تحمي الأجهزة غير التقليدية والأحادية الغرض والمتصلة بالإنترنت ضد التهديدات.  | حلول أمن إنترنت الأشياء والأجهزة المدمجة              | ٢-٩-١ |
| خدمات الأمن السيبراني الاحترافية           |   |   | ٢     |
| الاستشارات الإدارية في الأمن السيبراني     |   |   | ١-٢   |
| فئة الترخيص لتقديم الخدمة / المنتج أو الحل | الخدمات الاحترافية في الأمن السيبراني لتحديد مجالات التحسين الإستراتيجية وتقديم التوصيات.   |   |       |
| فئة الترخيص العام                          | الخدمات الاستشارية في الأمن السيبراني لوضع إستراتيجية الأمن السيبراني (مثل الرؤية والرسالة وغيرها) وخارطة طرق التنفيذ.  | تطوير إستراتيجية الأمن السيبراني وخارطة الطريق        | ١-١-٢ |
| فئة الترخيص العام                          | الخدمات الاستشارية في الأمن السيبراني لوضع السياسات والعمليات والإجراءات وأطر العمل في الأمن السيبراني بما يتماشى مع إستراتيجية الأمن السيبراني والمعايير الداخلية والخارجية للمنظمة. | تطوير سياسات وعمليات وإجراءات الأمن السيبراني         | ٢-١-٢ |
| فئة الترخيص العام                          | الخدمات الاستشارية في الأمن السيبراني لتطوير قدرات الأمن السيبراني في المنظمة بما يشمل الهيكل التنظيمي والأدوار والمسؤوليات والحوكمة وما إلى ذلك.                                     | تطوير نموذج قدرات الأمن السيبراني                     | ٣-١-٢ |
| فئة الترخيص العام                          | الخدمات الاستشارية في الأمن السيبراني لاعتماد الجهة مفعلاً لمعيار الاعتماد المعترف به خارجياً وبناءً على تقييم الأمن السيبراني.   | اعتماد وشهادات الأمن السيبراني للمنظمات               | ٤-١-٢ |
| فئة الترخيص العام                          | الخدمات الاستشارية في الأمن السيبراني التي تقدم إدارة التغيير وإدارة المشاريع في الأمن السيبراني باعتبارها جزء من تنفيذ المنتج/الحل وتحديثه وجزء من التحوّل في الأمن السيبراني.       | إدارة المشاريع وإدارة التغيير في مجال الأمن السيبراني | ٥-١-٢ |
| تقييم الالتزام السيبراني                   |   |   | ٢-٢   |
| فئة الترخيص لتقديم الخدمة / المنتج أو الحل | الخدمات الاحترافية في الأمن السيبراني لإجراء تقييمات الأمن السيبراني على مستوى الحوكمة، وبيئة تقنية المعلومات والتقنية التشغيلية في الجهة.  |   |       |

|  |   |  |       |
|--|---|--|-------|
| فئة الترخيص<br>المتخصص                           | خدمات تقييم الأمن السيبراني لتحليل سياسات الجهة وعملياتها وإجراءاتها وأطر عملها في الأمن السيبراني وتحديد نقاط الضعف وفرص التحسن.   | تقييم سياسات وعمليات وإجراءات الأمن السيبراني    | ١-٢-٢ |
| فئة الترخيص<br>المتخصص                           | خدمات تقييم الأمن السيبراني لتقييم قدرات الأمن السيبراني في الجهة بما يشمل الهيكل التنظيمي والأدوار والمسؤوليات والحوكمة وما إلى ذلك.   | تقييم نموذج قدرات الأمن السيبراني                | ٢-٢-٢ |
| فئة الترخيص<br>المتخصص                           | خدمات تقييم الأمن السيبراني لتقييم مدى نضج الأمن السيبراني في الجهة وفقاً لمعيار محدد وباستخدام نموذج تقييم النضج، مثل: تقييم مدى نضج الأمن السيبراني في الجهة وفقاً لضوابط الأمن السيبراني الصادرة من الهيئة، أو تقييم مدى نضج الأمن السيبراني في الجهة وفقاً لنماذج نضج مُعترف بها عالمياً. | تقييم نضج الأمن السيبراني                        | ٣-٢-٢ |
| فئة الترخيص<br>المتخصص                           | خدمات تقييم الأمن السيبراني للتحقق من الامتثال للأنظمة والضوابط والمعايير والأطر وغيرها الوطنية والعالمية الأخرى المتعلقة بالأمن السيبراني.   | تدقيق/تقييم الالتزام<br>بمتطلبات الأمن السيبراني | ٤-٢-٢ |
| تقييم المخاطر السيبرانية                         |   |  | ٣-٢   |
| فئة الترخيص<br>لتقديم الخدمة /<br>المنتج أو الحل | الخدمات الاحترافية في تقييم المخاطر التي يتم إجراؤها لتحديد مخاطر الأمن السيبراني وتحديد إجراءات معالجة التهديدات وعوامل تهديد الأمن.   |  |       |
| فئة الترخيص<br>المتخصص                           | خدمات تقييم المخاطر لتحديد مخاطر الأمن السيبراني في الجهة وتقييمها وترتيبها حسب الأولوية.   | تقييم المخاطر السيبرانية                         | ١-٣-٢ |
| فئة الترخيص<br>المتخصص                           | خدمات تقييم المخاطر لتوثيق المخاطر السيبرانية وإجراءات إدارة المخاطر في مستودع إدارة المخاطر.   | تطوير سجل مخاطر الأمن السيبراني                  | ٢-٣-٢ |
| التقييمات الفنية في الأمن السيبراني              |   |  | ٤-٢   |
| فئة الترخيص<br>لتقديم الخدمة /<br>المنتج أو الحل | الخدمات الاحترافية في الأمن السيبراني التي تقييم نواحي بيئة تقنية المعلومات والتقنية التشغيلية في الجهة.  |  |       |
| فئة الترخيص<br>المتخصص                           | الخدمات التقنية في الأمن السيبراني لتحديد الثغرات وتصنيفها وترتيبها حسب الأولوية في حل أو منظومة أو نظام أو شبكة محددة.   | تقييم الثغرات                                    | ١-٤-٢ |
| فئة الترخيص<br>المتخصص                           | الخدمات التقنية في الأمن السيبراني للعثور على الثغرات القابلة للاستغلال في حل أو منظومة أو نظام   | اختبار الاختراقات                                | ٢-٤-٢ |

|  |  |   |       |
|--|--|---|-------|
|  | أو شبكة محددة وإظهارها بشكل استباقي، واختبار مدى استغلالها.  |   |       |
| فئة الترخيص<br>المتخصص                           | الخدمات الفنية في الأمن السيبراني لتقييم مدى اكتمال الحلول وبنية الأمن السيبراني.  | مراجعة معمارية الأمن السيبراني                  | ٣-٤-٢ |
| فئة الترخيص<br>المتخصص                           | الخدمات الفنية في الأمن السيبراني لتحديد التهديدات غير المكتشفة إما بشكل استباقي (تصيد التهديدات) أو تفاعلي (تقييم الاختراق) استجابة إلى العثور على مؤشرات الاختراق (IoCs).  | خدمات تصيد التهديدات السيبرانية وتقييم الاختراق | ٤-٤-٢ |
| فئة الترخيص<br>المتخصص                           | الخدمات الفنية في الأمن السيبراني المستخدمة في هجمات المخترقون الأخلاقيون (الفريق الأحمر "Red Teaming") على أنظمة الجهة كمحاكات لتهديد سيبراني حقيقي، فيما يحاول مدافعو الجهة (الفريق الأزرق "Blue Teaming") الدفاع عن أنظمة وشبكة الجهة. وتشمل كذلك الاختبارات التي تجمع بين الفريق المهاجم والفريق المدافع (الفريق البنفسجي "Purple Teaming"). | خدمات الاختبارات لمحاكاة الهجمات السيبرانية     | ٥-٤-٢ |
| فئة الترخيص<br>المتخصص                           | الخدمات الفنية في الأمن السيبراني لتحديد العيوب والثغرات الأمنية في التطبيقات، مثل مراجعة شفرة المصدر واختبار أمن تطبيقات الأجهزة الذكية وما إلى ذلك.  | تقييم أمن التطبيقات                             | ٦-٤-٢ |
| فئة الترخيص<br>المتخصص                           | الخدمات التقنية للأمن السيبراني لمراجعة التكوين الأمني للأجهزة وتحديد التكوينات الخاطئة وفرص تعزيزها.  | مراجعة إعدادات الأمن السيبراني                  | ٧-٤-٢ |
| فئة الترخيص<br>المتخصص                           | الخدمات الفنية في الأمن السيبراني لتقييم الحل والمنتج (من أجهزة وبرمجيات) واعتماده وفقاً لمعايير اعتماد وطنية حسب ما يصدر عن الهيئة أو وفقاً لمعايير وشهادات مُعترف بها عالمياً.   | التقييم السيبراني والاعتماد للحلول والمنتجات    | ٨-٤-٢ |
| خدمات برامج مكافأة اكتشاف الثغرات (Bug Bounty)   |  |   | ٥-٢   |
| فئة الترخيص<br>لتقديم الخدمة /<br>المنتج أو الحل | الخدمات التقنية في الأمن السيبراني لتشغيل برنامج يحفز المخترقين الأخلاقيين لإجراء تقييمات مستقلة والإفصاح عن المسؤول.  |   |       |

|   |  |  |       |
|---|--|--|-------|
| فئة الترخيص<br>المتخصص  | الخدمات التقنية في الأمن السيبراني لتشغيل برنامج<br>يحفز المخترقين الأخلاقيين لإجراء تقييمات مستقلة<br>والإفصاح عن المسؤول.  | خدمات برامج مكافأة<br>اكتشاف الثغرات<br>(Bug Bounty) | ١-٥-٢ |
| الاستشارات التقنية في الأمن السيبراني   |  |  | ٦-٢   |
| فئة الترخيص<br>لتقديم الخدمة /<br>المنتج أو الحل  | الخدمات الاحترافية في الأمن السيبراني لتقديم التوصيات التقنية والأنشطة الاستشارية التقنية.   |  |       |
| فئة الترخيص العام   | الخدمات الفنية في الأمن السيبراني لتصميم البنية<br>الأمنية للجهة باستخدام أفضل الممارسات ومبادئ<br>التصميم الآمن.  | تصميم معمارية الأمن<br>السيبراني                     | ١-٦-٢ |
| فئة الترخيص العام   | الخدمات الفنية للأمن السيبراني لوضع معايير قابلة<br>للتنفيذ ومخصصة في الأمن السيبراني تتوافق مع<br>معايير القطاع، بما يشمل وضع الحد الأدنى من المعايير<br>الأمنية الأساسية (MBSS).                   | تطوير المعايير الفنية للأمن<br>السيبراني             | ٢-٦-٢ |
| فئة الترخيص العام   | الخدمات الفنية في الأمن السيبراني لإعداد الخطط<br>والعمليات التفصيلية، مثل استرداد البيانات الهامة<br>وخطة استمرارية الأعمال وخطة التخفيف من<br>المخاطر والثغرات وخطة الاستجابة للأحداث وغير<br>ذلك. | تطوير الخطة الفنية للأمن<br>السيبراني                | ٣-٦-٢ |
| الاستجابة والتحقيق في الحوادث السيبرانية  |  |  | ٧-٢   |
| فئة الترخيص<br>لتقديم الخدمة /<br>المنتج أو الحل  | الخدمات الاحترافية في الأمن السيبراني لتحليل ومعالجة الحوادث والاختراقات في الأمن السيبراني.   |  |       |
| فئة الترخيص<br>المتخصص<br><small>(يتم ترخيص هذه الخدمة لمستوى واحد<br/>فقط (متخصص-١))</small> | خدمات الاستجابة لحوادث الأمن السيبراني لمساعدة<br>الجهات في إدارة حوادث الأمن السيبراني وتحليلها<br>واحتوائها ومعالجتها والتعلم منها.  | الاستجابة للحوادث السيبرانية                         | ١-٧-٢ |
| فئة الترخيص<br>المتخصص<br><small>(يتم ترخيص هذه الخدمة لمستوى واحد<br/>فقط (متخصص-١))</small> | خدمات التحقيق الجنائي في حوادث الأمن السيبراني<br>لحفاظ على الأدلة وتحليل تقنيات الجهات التخريبية<br>وعوامل التهديدات (مثل: تحليل البرامج الضارة).   | التحليل الجنائي في الأمن<br>السيبراني                | ٢-٧-٢ |

|   |   |   |              |
|---|---|---|--------------|
| <p>فئة الترخيص<br/>المتخصص</p> <p><small>(يتم ترخيص هذه الخدمة لمستوى واحد فقط (متخصص-1))</small></p> | <p>الخدمات الفنية في الأمن السيبراني لتقديم المعلومات والتقارير لاستيعاب النوايا والأهداف وتقنيات الهجوم للجهات التخريبية وعوامل التهديدات (بما يشمل (Dark Web) والعلامة التجارية ومراقبة التهديدات السيبرانية)، وتحليلها وفحصها.</p> | <p>خدمات المعلومات الاستباقية عن التهديدات السيبرانية</p> | <p>٢-٧-٣</p> |
| <p>خدمات التنفيذ التقني للأمن السيبراني</p>   |   |   | <p>٣</p>     |
| <p>تطوير منتجات وحلول الأمن السيبراني</p>   |   |   | <p>١-٣</p>   |
| <p>فئة الترخيص<br/>لتقديم الخدمة /<br/>المنتج أو الحل</p>   | <p>خدمات الأمن السيبراني لتطوير منتجات الأمن السيبراني وحلوله.</p>  |   |              |
| <p>فئة الترخيص العام</p>  | <p>الخدمات الفنية للأمن السيبراني لتطوير منتجات وحلول مخصصة للأمن السيبراني لموردي الخدمات التقنية والجهات الوطنية وغيرها من المستخدمين المتقدمين.</p>  | <p>تطوير منتجات وحلول الأمن السيبراني</p>                 | <p>١-١-٣</p> |
| <p>تكامل أنظمة الأمن السيبراني</p>  |   |   | <p>٢-٣</p>   |
| <p>فئة الترخيص<br/>لتقديم الخدمة /<br/>المنتج أو الحل</p>   | <p>خدمات الأمن السيبراني المقدمة من موردي الأمن السيبراني وموردي تقنية المعلومات وشركات تكامل الأنظمة لتنفيذ حل الأمن السيبراني أو إعداده.</p>  |   |              |
| <p>فئة الترخيص العام</p>  | <p>الخدمات الفنية للأمن السيبراني لتحديد متطلبات الأمن السيبراني لمنتجات أو حلول الأمن السيبراني الجديدة ولتنفيذ منتج أو حل الأمن السيبراني.</p>  | <p>متطلبات الأمن السيبراني لتنفيذ الحلول</p>              | <p>١-٢-٣</p> |
| <p>فئة الترخيص العام</p>  | <p>الخدمات الفنية في الأمن السيبراني لتصميم بنية الأمن السيبراني للحل قبل تنفيذه باستخدام أفضل الممارسات ومبادئ التصميم الآمن (بما يشمل التصميم العام والتفصيلي).</p>   | <p>معمارية وتصميم حلول الأمن السيبراني</p>                | <p>٢-٢-٣</p> |

|   |  |  |       |
|---|--|--|-------|
| فئة الترخيص العام   | الخدمات الفنية في الأمن السيبراني لتنفيذ حلول الأمن السيبراني وإعدادها ودمجها ضمن بيئة الجهة بما يشمل عقود الصيانة والدعم للمنتج أو الحل.  | تنفيذ وإعداد وتكامل حلول الأمن السيبراني         | ٣-٢-٣ |
| الخدمات المدارة للأمن السيبراني   |  |  | ٤     |
| إدارة مركز عمليات الأمن السيبراني   |  |  | ١-٤   |
| حسب الموضح في الإطار التنظيمي لترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدار. |  |  |       |
| حلول الأمن السيبراني كخدمة  |  |  | ٢-٤   |
| فئة الترخيص لتقديم الخدمة / المنتج أو الحل  | خدمات الأمن السيبراني المتصلة بالإسناد الخارجي لحلول الأمن السيبراني، بما يشمل إدارة الحلول والعمليات.   |  |       |
| فئة الترخيص العام   | خدمات الإسناد الخارجي في الأمن السيبراني التي تتيح التحكم في العمليات اليومية وتنفيذ حلول الأمن السيبراني، بما في ذلك إدارة الحلول والعمليات، باستثناء مركز العمليات الأمنية المُدارة، والاستجابة إلى الحوادث. | حلول الأمن السيبراني كخدمة                       | ١-٢-٤ |
| الإسناد الخارجي للقوى العاملة في الأمن السيبراني                                      |  |  | ٣-٤   |
| فئة الترخيص لتقديم الخدمة / المنتج أو الحل  | خدمات الأمن السيبراني المتصلة بإسناد القوى العاملة في الأمن السيبراني إلى الجهات.  |  |       |
| فئة الترخيص العام   | خدمات الإسناد الخارجي في الأمن السيبراني التي تقدم المتعاقدين لسد النقص في موظفين الأمن السيبراني في الجهة، باستثناء أنشطة الاستجابة إلى الحوادث.  | الإسناد الخارجي للقوى العاملة في الأمن السيبراني | ١-٣-٤ |
| خدمات التدريب وبناء القدرات في الأمن السيبراني  |  |  | ٥     |
| التدريب في مجال الأمن السيبراني   |  |  | ١-٥   |
| فئة الترخيص لتقديم الخدمة / المنتج أو الحل  | تقديم دورات تدريبية وورش عمل في الأمن السيبراني لموظفي الأمن السيبراني وغيرهم.   |  |       |
| فئة الترخيص العام   | خدمات التدريب في الأمن السيبراني التي تركز على المفاهيم والنظرية والإدارة في الأمن السيبراني.  | التدريب الأكاديمي في الأمن السيبراني             | ١-١-٥ |

|  |  |  |       |
|--|--|--|-------|
| فئة الترخيص العام                          | خدمات التدريب في الأمن السيبراني التي تركز على الخبرات العملية في الأمن السيبراني بالأدوات والتقنيات التطبيقية.  | التدريب الفني في الأمن السيبراني                             | ٢-١-٥ |
| فئة الترخيص العام                          | خدمات التدريب في الأمن السيبراني التي تركز على التدريب على نهج الكشف عن حوادث الأمن السيبراني والاستجابة لها ومعالجتها.  | تمارين وعمليات المحاكاة في الأمن السيبراني                   | ٣-١-٥ |
| التوعية في مجال الأمن السيبراني            |  |  | ٢-٥   |
| فئة الترخيص لتقديم الخدمة / المنتج أو الحل | تقديم الدورات التوعوية وورش عمل لموظفي الأمن السيبراني وغيرهم.   |  |       |
| فئة الترخيص العام                          | خدمات التوعية بالأمن السيبراني التي تركز على إنشاء المحتويات المخصصة لتحسين مستوى الوعي والفهم لدى الموظفين والعملاء وغيرهم في موضوع الأمن السيبراني.          | تطوير محتوى التوعية في مجال الأمن السيبراني                  | ١-٢-٥ |
| فئة الترخيص العام                          | خدمات التوعية بالأمن السيبراني التي تركز على تقديم الدورات التوعوية المباشرة أو عن بعد في الأمن السيبراني للموظفين والعملاء وغيرهم.                            | الدورات التدريبية وورش العمل للتوعية في مجال الأمن السيبراني | ٢-٢-٥ |
| اختبارات وشهادات الأمن السيبراني           |  |  | ٣-٥   |
| فئة الترخيص لتقديم الخدمة / المنتج أو الحل | إجراء الاختبارات وتقديم الشهادات في الأمن السيبراني للأفراد.   |  |       |
| فئة الترخيص العام                          | خدمات إجراء الاختبارات في الأمن السيبراني لاختبار معارف الطلاب والمتخصصين في الأمن السيبراني ومهاراتهم وكفاءاتهم.  | اختبارات الأمن السيبراني للأفراد                             | ١-٣-٥ |
| فئة الترخيص العام                          | خدمات الاعتماد في الأمن السيبراني للتحقق من التدريب أو الخبرات واعتماد الأفراد من خلال تقديم شهادات معترف بها في الأمن السيبراني (بما يشمل الشهادات المعادلة). | الشهادات الاحترافية في الأمن السيبراني للأفراد               | ٢-٣-٥ |
| الفعاليات والمسابقات في الأمن السيبراني    |  |  | ٤-٥   |

| فئة الترخيص لتقديم الخدمة / المنتج أو الحل | إقامة الفعاليات والمسابقات في الأمن السيبراني للجهات.  |   |       |
|--|--|---|-------|
| فئة الترخيص العام                          | خدمات الأمن السيبراني لتخطيط الفعاليات والمؤتمرات والمنتديات في الأمن السيبراني وتنظيمها وتنفيذها.                                     | الفعاليات في الأمن السيبراني                | ١-٤-٥ |
| فئة الترخيص العام                          | خدمات الأمن السيبراني التي من شأنها التخطيط لمسابقات الأمن السيبراني وتنظيمها وإجراءها مثل الهاكاثونات ومسابقات الأمن السيبراني (CTF). | المسابقات والتحديات في مجال الأمن السيبراني | ٢-٤-٥ |

## الملحق (ب): جدول المقابلات المالية لطلب ترخيص تقديم خدمات أو منتجات أو حلول الأمن السيبراني

- يجب على مقدم الطلب، بموجب هذا الإطار؛ سداد المقابل المالي على النحو المقرر في هذا الملحق لطلب الحصول على الترخيص أو تجديده. وتحتفظ الهيئة بالحق في إجراء التعديلات التي تراها على هذا المقابل المالي و/ أو فرض مقابلات مالية أخرى على المرخص له.
- تكون جميع المقابلات المالية المدفوعة - بموجب هذا الملحق - غير مستردة.
- يبين الجدول الآتي المقابلات المالية لطلب الحصول على ترخيص تقديم خدمات أو منتجات أو حلول الأمن السيبراني، وتجديده والمحافظة عليه بموجب هذا الإطار:

| المقابل المالي بحسب حجم منشأة مقدم طلب الترخيص ويحدد حجم المنشأة وفق تعريف الهيئة العامة للمنشآت الصغيرة والمتوسطة (منشآت) |              |              |               | الوصف  | فئة الترخيص                          |
|--|--------------|--------------|---------------|--|--------------------------------------|
| كبيرة  | متوسطة       | صغيرة        | متناهية الصغر |  |                                      |
| ١,٠٠٠,٠٠٠ ريال   | ٥٠٠,٠٠٠ ريال | ٣٠٠,٠٠٠ ريال | لا ينطبق      | مقابل مالي عند تقديم الطلب، وسنوياً خلال مدة سريان الترخيص (لكل مجال فرعي) | المتخصص - المستوى الأول (متخصص - ١)  |
| ٥٠٠,٠٠٠ ريال   | ٣٠٠,٠٠٠ ريال | ٢٠٠,٠٠٠ ريال | ١٥٠,٠٠٠ ريال  |  | المتخصص - المستوى الثاني (متخصص - ٢) |
| ٥٠,٠٠٠ ريال  |              |              |               | مقابل مالي لطلب الحصول على الترخيص أو التجديد لفئة العام                   | العام - كافة المستويات               |

مبادئ العموم