الإطار التنظيمي لتقديم خدمات الأمن السيبراني في جمهورية مصر العربية

يونيو ٢٠٢٤

المحتوى

تمهيد

لما كان الجهاز القومي لتنظيم الاتصالات هو الجهة المنوطة بتنظيم قطاع الاتصالات بما يضمن حماية حقوق المستخدمين من جهات حكومية وشركات وأفراد مع الحفاظ على سرية وتأمين خدمات الاتصالات.

ولما كان القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات قد حدد التزامات مقدمي خدمات تكنولوجيا المعلومات والاتصالات وذلك بما يضمن حماية البيانات والمعلومات والأنظمة والشبكات المعلوماتية، كما يعتبر الجهاز أحد الجهات الرئيسية المنوطة بإنفاذ أحكام هذا القانون على مقدمي خدمات تقنية المعلومات والاتصالات.

وطبقاً للقانون رقم ١٠ لسنة ٢٠٠٣ بشأن تنظيم الاتصالات فإن الجهاز منوط بتحديد الأسس العامة التي يلتزم بها مشغلو ومقدمو خدمات الاتصالات لضمان تأمين البنية التحتية وسرية البيانات الخاصة بعملاء تلك الخدمات، وحيث أن وضع القواعد اللازمة للتأكد من تقديم خدمات الأمن السيبراني للشركات المرخص لها بتقديم خدمات الاتصالات في جمهورية مصر العربية هو أحد آليات تحقيق ذلك.

وحيث أن المجلس الأعلى للأمن السيبراني طبقاً لقرار رئيس مجلس الوزراء رقم ١٦٣٠ بتاريخ ٢٠١٦ هو الجهة المختصة بتحديد البنية التحتية الحرجة للاتصالات وتكنولوجيا المعلومات لكافة قطاعات الدولة سواء القطاع العام أو القطاع الخاص، واعتماد سياسات واستراتيجيات تأمين تلك البنية التحتية بالإضافة إلى وضع المعايير اللازمة لكافة الجهات كحد أدنى لتأمين البنية التحتية الحرجة.

ونفاذً لقرار رئيس مجلس الوزراء رقم ٩٩٤بتاريخ ٢٠١٧ والذي ينص على إلزام كافة الجهات الحكومية وشركات قطاع الأعمال بتنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني فيما يتعلق بتأمين البنية التحتية الحرجة للاتصالات وتكنولوجيا المعلومات واتخاذ كافة الإجراءات الفنية والإدارية اللازمة في هذا الشأن.

وفي ضوء ازدياد الطلب على خدمات الأمن السيبراني والتطور الذي شهدته تلك الخدمات من تقييم المخاطر ونقاط الضعف في الأنظمة وإدارة وتطوير برامج الأمان وغيرها مما يستلزم وضع معايير وضوابط للتأكد من توافر الخبرات والكفاءة الفنية اللازمة للشركات مقدمي خدمات الأمن السيبراني تحقيقاً لأهداف حماية وتأمين خدمات الاتصالات وتكنولوجيا المعلومات والبنية التحتية المعلوماتية للقطاعين العام والخاص في جمهورية مصر العربية.

فقد قرر الجهاز القومي لتنظيم الاتصالات إصدار الإطار التنظيمي الماثل الذي ينظم عمل مقدمي خدمات الأمن السيبراني من خلال تحديد الضوابط الفنية والتنظيمية اللازمة لتقديم تلك الخدمات في جمهورية مصر العربية.

أولاً

التعريفات

١-١ **الجهاز:** يقصد به الجهاز القومي لتنظيم الاتصالات.

١-٢ **المجلس:** يقصد به المجلس الأعلى للأمن السيبراني.

١-٣ **البنية التحتية المعلوماتية الحرجة:** يقصد بها مجموعة أنظمة أو شبكات أو أصول معلوماتية أساسية يؤدى الكشف عن تفصيلاتها تعطيلها أو تغيير طريقة عملها بطريقة غير مشروعة، أو الدخول غير المصرح به عليها، أو الدخول أو الوصول بشكل غير قانوني للبيانات والمعلومات التي تحفظها أو تعالجها، أو يؤدى القيام بأي فعل غير مشروع آخر بها إلى التأثير على توافر خدمات الدولة ومرافقها الأساسية أو خسائر اقتصادية أو اجتماعية كبيرة على المستوى الوطني، وتشمل هذه البنية التحتية الحرجة القطاعات المحددة في المرفق رقم (٢) من الإطار الماثل.

١-٤ **خدمات الأمن السيبراني:** يقصد بها الخدمات التي تقدم للغير بغرض (تحديد ورصد) التهديدات الرقمية للأنظمة والشبكات و/أو توفير (الحماية) اللازمة لتأمين وسلامة تشغيلها و/أو توفير (الاستجابة) لإزالة التهديدات و/أو (استعادة) التشغيل للأنظمة والشبكات حال توقفها عن العمل بسبب حوادث نتجت عن تلك التهديدات، وتشمل الخدمات المحددة بالملحق (١) وما قد يقره الجهاز مستقبلاً من خدمات.

١-٥ **الجهات المستفيدة (الفئة الأولى):** يقصد بها الجهات أو الشركات التي تتعاقد مع أحد مقدمي خدمات الأمن السيبراني بغرض الحصول على خدماتهم وتشمل الفئات التالية:

- الجهات الحكومية وشركات قطاع الأعمال
- شركات القطاع الخاص التي (تحوز/تشغل) بنية تحتية حرجة للاتصالات وتكنولوجيا المعلومات
- شركات الاتصالات المرخص لها في جمهورية مصر العربية

١-٦ **الجهات المستفيدة (الفئة الثانية):** يقصد بها شركات القطاع الخاص التي لا (تحوز/تشغل) بنية تحتية حرجة للاتصالات وتكنولوجيا المعلومات والتي تتعاقد مع أحد مقدمي خدمات الأمن السيبراني بغرض الحصول على خدمات الأمن السيبراني.

١-٧ **مقدمي خدمات الأمن السيبراني:** يقصد بهم أي شخص اعتباري مسجل لدى الجهاز بغرض تقديم خدمات الأمن السيبراني للغير من الجهات المستفيدة ويشمل:

- **مقدمي خدمات الأمن السيبراني (المستوى الأول):** مقدمي خدمات الأمن السيبراني للغير من الجهات المستفيدة (الفئة الأولى والثانية).
- **مقدمي خدمات الأمن السيبراني (المستوى الثاني):** مقدمي خدمات الأمن السيبراني للغير من الجهات المستفيدة (من الفئة الثانية فقط).

١-٨ **شهادة تسجيل الأمن السيبراني (شهادة التسجيل):** يقصد بها الشهادة الصادرة من الجهاز للأشخاص الاعتباريين بغرض تقديم خدمات الأمن السيبراني للجهات المستفيدة من الفئة الأولى أو الثانية.

١-٩ **شهادة اعتماد الأمن السيبراني (شهادة الاعتماد):** يقصد بها الشهادة الصادرة من الجهاز للأشخاص الطبيعيين (أفراد) بغرض تقديم خدمات الأمن السيبراني للجهات المستفيدة من الفئة الأولى أو الثانية.

١-١٠ **سجل مقدمي خدمات الأمن السيبراني:** يقصد به قائمة الشركات مقدمي خدمات الامن السيبراني المسجلين والافراد المعتمدين التي ينشرها ويحدثها الجهاز.

ثانياً

نطاق تطبيق الإطار التنظيمي

٢-١ يخضع لشروط وأحكام الإطار التنظيمي الماثل كل من:

- أي شخص طبيعي أو اعتباري يقوم بتقديم خدمات الأمن السيبراني لأي جهة مستفيدة داخل جمهورية مصر العربية.
- الجهات المستفيدة من الفئة الأولى أو الثانية داخل جمهورية مصر العربية.

٢-٢ يسري الإطار التنظيمي الماثل من تاريخ ٢٠٢٤/٨/٦. وعلى أي شخص طبيعي أو اعتباري يقوم بتقديم خدمات الأمن السيبراني والجهات المستفيدة بفئتيها توفيق أوضاعها خلال عام من تاريخ صدوره وفقاً للإجراءات المحددة به.

ثالثاً

النموذج التنظيمي لخدمات الأمن السيبراني

٣-١ تلتزم الشركات الراغبة/العاملة في تقديم خدمات الأمن السيبراني لأي جهة مستفيدة داخل جمهورية مصر العربية بالحصول على شهادة التسجيل من الجهاز لتقديم خدمات الأمن السيبراني وفقاً للإجراءات والشروط المحددة في هذا الشأن.

٣-٢ يلتزم مقدمو خدمات الأمن السيبراني لأي جهة مستفيدة داخل جمهورية مصر العربية بإتباع الإجراءات الخاصة باعتماد الأفراد العاملين لديهم في تقديم الخدمة وفقاً للإجراءات والشروط المحددة في هذا الشأن، ولا يجوز للأفراد المعتمدين تقديم خدمات الامن السيبراني بشكل فردى ويجب انتمائهم وظيفياً لأحد مقدمي خدمات الامن السيبراني المسجلين.

٣-٣ يجوز للجهات المستفيدة تقديم خدمات الأمن السيبراني لنفسها ودون تقديمها للغير وذلك بعد الحصول على موافقة كتابية مسبقة من الجهاز بشرط اعتماد الأفراد العاملين لديها في مجال الأمن السيبراني وفقاً لما يصدره الجهاز من إجراءات ومحددات في هذا الشأن.

٣-٤ يصدر الجهاز شهادات تسجيل الشركات بغرض تقديم خدمات الأمن السيبراني، كما يصدر شهادات الاعتماد للأفراد طبقاً للإجراءات المحددة في البندين سادساً وسابعاً من الإطار الماثل.

٣-٥ مدة شهادة التسجيل/الاعتماد ٣ أعوام من تاريخ صدورها، ويجوز تجديدها لمدد أخرى كلاً منها ٣ أعوام وذلك وفقاً للشروط والإجراءات التي يحددها الجهاز في هذا الشأن.

٣-٦ يحق للجهاز خلال مدة صلاحية شهادة التسجيل/الاعتماد الغاء الشهادة أو حذف مقدم الخدمة او حذف الافراد المعتمدين لفترة زمنية من سجل مقدمي خدمات الأمن السيبراني المعلن في حالة الإخلال بأي من التزاماته الفنية أو التنظيمية.

٣-٧ في حالة مخالفة الأفراد المعتمدين من الجهاز لأي من متطلبات الاعتماد أو لقواعد ولوائح وسياسات وأطر ومعايير الأمن السيبراني الصادرة من المجلس الأعلى للأمن السيبراني، يجوز للجهاز وقف/إلغاء شهادة الاعتماد.

٣-٨ يقوم الجهاز بنشر وتحديث سجل مقدمي خدمات الأمن السيبراني وذلك على الموقع الرسمي للجهاز.

٣-٩ يخضع تقديم خدمات الأمن السيبراني للقوانين المصرية السارية وعلى الأخص قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ وقانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية.

٣-١٠ يلتزم مقدمو خدمات الأمن السيبراني والأفراد المعتمدين من الجهاز والجهات المستفيدة بالقرارات والأطر والمعايير والضوابط والإرشادات والأنظمة المتعلقة بالأمن السيبراني والقرارات ذات الصلة التي يصدرها الجهاز القومي لتنظيم الاتصالات والمجلس الأعلى للأمن السيبراني وما يستجد عليها.

٣-١١ يحق للجهاز تعديل مقابل إصدار وتجديد شهادة التسجيل/الاعتماد ويلتزم مقدمي خدمات الأمن السيبراني والافراد المعتمدين بسداد المقابل وفقاً لهذا التعديل (إن وجد).

رابعاً

التزامات مقدمي خدمات الأمن السيبراني

٤-١ يلتزم مقدمو خدمات الأمن السيبراني بقواعد ولوائح وسياسات وأطر ومعايير الأمن السيبراني الصادرة من المجلس الأعلى للأمن السيبراني في هذا الشأن، وفي حالة مخالفة ذلك يتم إخطار مقدمي خدمات الأمن السيبراني من قبل الجهاز والتنبيه على إزالة المخالفة وفقاً لإطار زمني يحدده الجهاز يتناسب مع حجم المخالفة وذلك كله مع عدم الإخلال بأحكام القانون رقم ١٠ لسنة ٢٠٠٣ بشأن تنظيم الاتصالات وأحكام القانون رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية.

٤-٢ في حالة عدم إزالة المخالفة وفقاً لتعليمات الجهاز، يتم تطبيق أحكام القانون رقم ١٠ لسنة ٢٠٠٣ بشأن تنظيم الاتصالات وأحكام القانون رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية بشأن مكافحة جرائم تقنية المعلومات على مقدمي خدمات الأمن السيبراني و/أو إيقاف أو إلغاء شهادة التسجيل.

٤-٣ يلتزم مقدمو خدمات الأمن السيبراني باستيفاء متطلبات الجهاز المحددة بالبند (سابعاً: متطلبات اعتماد الافراد) بشأن اعتماد العاملين لديه في تقديم خدمات الأمن السيبراني وذلك طبقاً لتعليمات الجهاز.

٤-٤ يحظر على مقدمي خدمات الأمن السيبراني تقديم أي من خدمات الأمن السيبراني للجهات المستفيدة غير تلك الخدمات المحددة في شهادة التسجيل الصادرة لهم.

٤-٥ يحظر على مقدمي خدمات الامن السيبراني تقديم خدمات الأمن السيبراني الا لفئة العملاء المصرح لهم بها وفقاً لشهادة التسجيل الصادرة من الجهاز.

٤-٦ يلتزم مقدمو خدمات الامن السيبراني بإخطار عملائهم مستوى شهادة التسجيل الصادرة من الجهاز قبل إبرام العقود الخاصة بتقديم خدمات الامن السيبراني.

٤-٧ يلتزم مقدمو خدمات الأمن السيبراني بإخطار الجهات المستفيدة بأي تغير يطرأ على شهادة التسجيل.

٤-٨ يلتزم مقدمو خدمات الأمن السيبراني والعاملون لديهم بالمحافظة على سرية وخصوصية ما يحصلون عليه من معلومات أو بيانات أو تقارير أياً كانت طبيعتها تكون متعلقة بتقديم الخدمة وعدم إذاعة محتواها بأي وسيلة كلياً أو جزئياً. كما يلتزم مقدمي خدمات الأمن السيبراني بعدم البدء في تقديم أي من الخدمات قبل إبرام اتفاقية عدم الإفصاح Non-disclosure Agreement مع الجهة المستفيدة.

٤-٩ يلتزم مقدم خدمات الأمن السيبراني بالإمساك والاحتفاظ بصورة مؤمنة للبيانات والتقارير الخاصة بالخدمة لمدة لا تقل عن سنة، كما يلتزم بتأمين تلك البيانات بما يحافظ على سريتها وسلامتها وعدم تسريبها أو تلفها.

٤-١٠ **في حالة تقديم خدمات التقييم الأمني**، يلتزم مقدمو خدمات الأمن السيبراني بتقديم تقرير فني تقييمي للأمن السيبراني للجهاز سنوياً وكذلك فور حدوث تغيرات كبيرة وهامة في التطبيقات أو الأجهزة الخاصة بالخدمة أو حين يُطْلَب منه ذلك بشكل فوري على أن يتضمن هذا التقرير اختبارات الاختراقات والاختبارات الخاصة بنقاط الضعف.

٤-١١ يحق للجهاز أو من يفوضه إجراء عمليات تدقيق معلنة للأمن السيبراني (Announced Cybersecurity Audit) ويلتزم كل من مقدمي خدمات الأمن السيبراني والجهات المستفيدة بالتعاون مع الجهاز وأن يضع تحت تصرف الجهاز أو من يفوضه الدفاتر/السجلات الإلكترونية وأي بيانات يراها ضرورية ولازمة عند إجراء عملية تقييم تأمين الخدمة، ويتم إخطار مقدمي خدمات الأمن السيبراني قبل عملية التدقيق بمدة لا تقل عن شهر.

٤-١٢ يحق للجهاز أو من يفوضه إجراء عمليات تدقيق غير معلنة للأمن السيبراني (Unannounced Cybersecurity Audit)ويلتزم كل من مقدمي خدمات الأمن السيبراني والجهات المستفيدة بأن يضعوا تحت تصرف الجهاز أو من يفوضه في ذلك جميع الدفاتر/السجلات الإلكترونية وأن يسمح له أو لمن يفوضه بالاطلاع عليها وأخذ أي بيانات يراها ضرورية ولازمة عند إجراء عملية تقييم تأمين الخدمة.

٤-١٣ يلتزم مقدمو خدمات الأمن السيبراني بموافاة الجهاز بما يطلبه من بيانات ومستندات وإيضاحات تتعلق بالأمن السيبراني في الموعد وبالشكل الذي يحدده الجهاز، كما يلتزم مقدمو خدمات الأمن السيبراني بدقة وصحة هذه البيانات.

٤-١٤ يحظر على مقدمي خدمات الأمن السيبراني التوقف عن تقديم خدماتهم المحددة بشهادة التسجيل إلا بعد الحصول على موافقة مسبقة من الجهاز وإخطار عملائهم قبل التوقف عن تقديم الخدمة بمدة لا تقل عن ستة أشهر.

٤-١٥ يلتزم مقدمو خدمات الأمن السيبراني بالحصول على الموافقة الكتابية المسبقة من الجهاز في حالة حدوث أي تغيير في الشكل القانوني أو النسب المئوية لمساهمي مقدمي خدمات الأمن السيبراني.

٤-١٦ يلتزم مقدمو خدمات الأمن السيبراني – في نطاق الخدمات المقدمة لعملائهم من الجهات المستفيدة – بإبلاغ الجهاز دون تأخير عن أي حوادث تتعلق بالأمن السيبراني أو تسريب البيانات.

خامساً

التزامات الجهات المستفيدة

٥-١ يحظر على الجهة المستفيدة التعاقد للحصول على خدمات الأمن السيبراني مع الأفراد أو الكيانات الغير حاصلة على شهادة التسجيل من الجهاز، كما تلتزم باتخاذ كافة التدابير التعاقدية لضمان تحقيق ذلك.

٥-٢ تلتزم الجهة المستفيدة بإخطار الجهاز فور حدوث أي حوادث تتعلق بالأمن السيبراني من خلال تقديم تقرير للجهاز خلال ٤٨ ساعة عن وصف المشكلة وحجم العملاء المتأثرين ومدة تأثرهم والإجراءات التي تم اتخاذها للتعامل مع هذه المشكلة وتلافيها مستقبلاً.

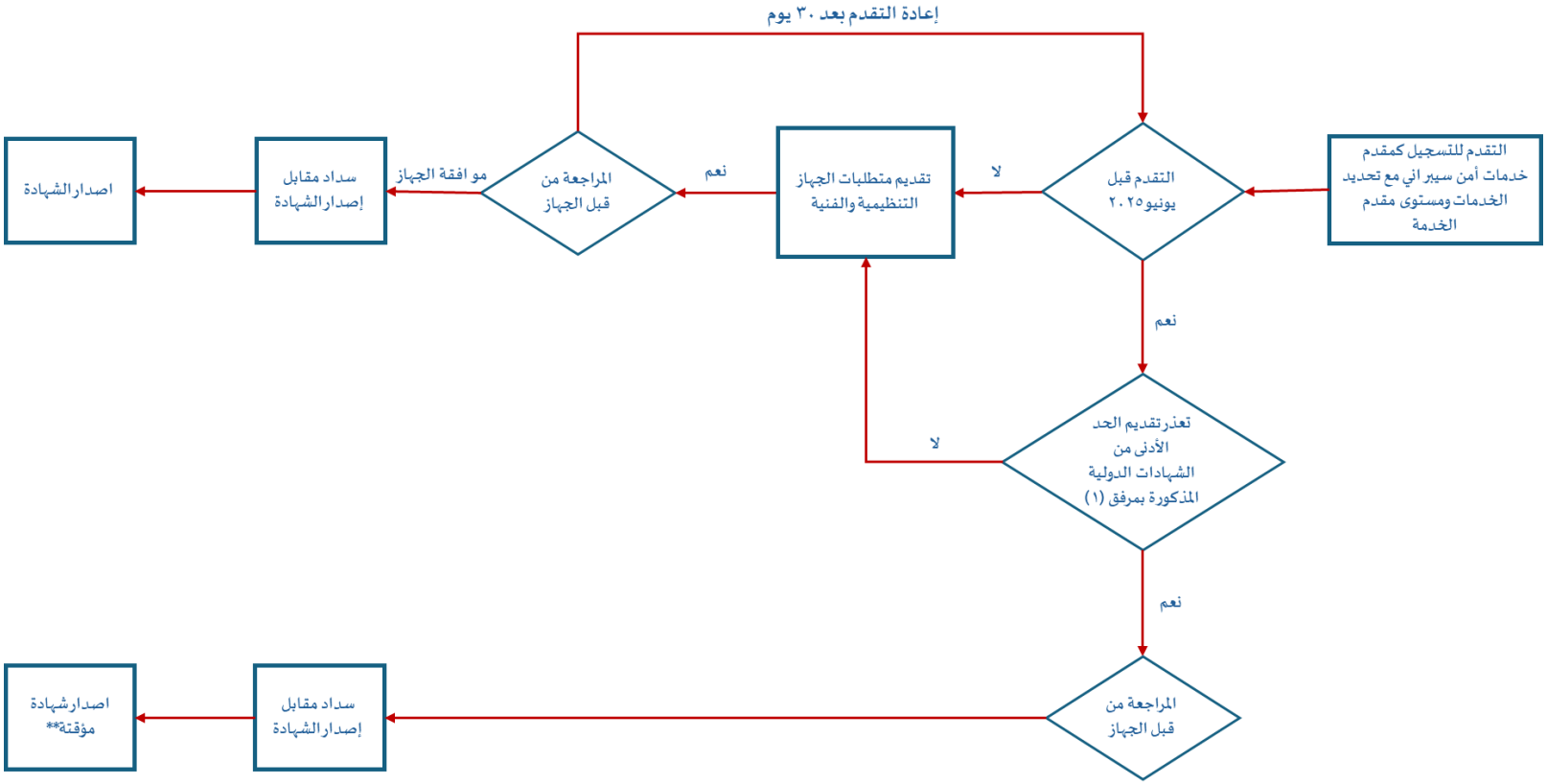
٥-٣ في حالة تبين وجود ثغرات تلتزم الجهة المستفيدة بالإصلاح الفوري أو إيقاف الخدمة محل الثغرة لحين الإصلاح وذلك كله طبقاً لتعليمات الجهاز.

٥-٤ تلتزم الجهة المستفيدة بموافاة الجهاز بما يطلبه من بيانات ومستندات وإيضاحات تتعلق بالأمن السيبراني في الموعد وبالشكل الذي يحدده الجهاز، كما تلتزم الجهة المستفيدة بدقة وصحة هذه البيانات.

٥-٥ يحظر على الجهة المستفيدة من الفئة الأولى التعاقد على خدمات الأمن السيبراني مع مقدمي خدمات الأمن السيبراني من المستوى الثاني.

سادساً

إجراءات تسجيل مقدمي خدمات الأمن السيبراني



*يشترط استيفاء جميع متطلبات الجهاز التنظيمية

**يتم اصدار شهادة مؤقتة وعلى مقدم الخدمة الالتزام بتقديم الحد الادنى من الشهادات الدولية خلال مدة عام من تاريخ الاصدار

في حالة توافر المتطلبات والشهادات الدولية للخدمات المطلوبة

- التقدم بطلب للحصول على شهادة التسجيل وسداد المقابل المقرر لذلك على أن يتضمن الطلب المستندات التالية:
  - نوع الخدمات المطلوب تقديمها والمنصوص عليها في ملحق (١) وما يستجد عليه.
  - تحديد مستوى مقدم الخدمة.
  - هيكل الشركة وموقفها المالي وقائمة المساهمين.
  - سابقة الأعمال والخبرات المحلية والدولية وقائمة بكافة العملاء الحاليين.
  - الشهادات والاعتمادات الفنية من الجهات المختلفة مع تحديد تلك الجهات وتاريخ الحصول على تلك الشهادات أو الاعتمادات ومدة صلاحيتها.
  - أي بيانات أو ايضاحات يطلبها الجهاز في عملية التقييم.
- يقوم الجهاز بدراسة الطلبات المقدمة من الشركات خلال ٩٠ يوم من تاريخ تقديم الطلب للجهاز بشرط استيفاء كافة البيانات التي يطلبها الجهاز لدراسة الطلبات،
- في حالة قبول طلب الشركة، يتم سداد مقابل إصدار شهادة التسجيل طبقاً لجدول مقابل إصدار شهادة التسجيل وتقديم اشعار السداد.
- يتم إصدار شهادة التسجيل وتكون سارية لمدة ٣ سنوات من تاريخ إصدارها.

في حالة عدم توافر المتطلبات والشهادات الدولية للخدمات المطلوبة (حتى يونيو ٢٠٢٥)

- التقدم بطلب للحصول على شهادة التسجيل وسداد المقابل المقرر لذلك على أن يتضمن الطلب المستندات التالية:
  - نوع الخدمات المطلوب تقديمها والمنصوص عليها في ملحق (١) وما يستجد عليه.
  - تحديد مستوى مقدم الخدمة.
  - هيكل الشركة وموقفها المالي وقائمة المساهمين.
  - سابقة الأعمال والخبرات المحلية والدولية وقائمة بكافة العملاء الحاليين.
  - الشهادات والاعتمادات الفنية من الجهات المختلفة مع تحديد تلك الجهات وتاريخ الحصول على تلك الشهادات أو الاعتمادات ومدة صلاحيتها.
  - أي بيانات أو ايضاحات يطلبها الجهاز في عملية التقييم.
- يقوم الجهاز بدراسة الطلبات المقدمة من الشركات خلال ٩٠ يوم من تاريخ تقديم الطلب للجهاز بشرط استيفاء كافة البيانات المحددة لدراسة الطلبات،
- في حالة قبول طلب الشركة، يتم سداد مقابل إصدار شهادة التسجيل المؤقتة طبقاً لجدول مقابل إصدار شهادة التسجيل وتقديم أشعار السداد.
- يتم إصدار شهادة تسجيل مؤقتة على أن يلتزم مقدم الخدمة بتقديم الشهادات الدولية خلال مدة لا تتعدى عام واحد من تاريخ إصدار الشهادة المؤقتة، وفى حالة عدم تقديم الشهادات الدولية خلال الفترة المحددة يلتزم بإيقاف تقديم الخدمات وفقاً لتعليمات الجهاز.

مقابل إصدار/تجديد شهادة التسجيل (المستوى الأول)

الخدمات		المقابل (جنيه مصري)		
		طلب الحصول على شهادة التسجيل	إصدار أو تجديد شهادة التسجيل	إصدار الشهادة المؤقتة
خدمات التقييم الأمني	اختبارات الاختراق (Penetration Testing)	٢٠٠٠	١٢٥٠٠٠	٤٠٠٠٠
	خدمات الفريق الأحمر (Red teaming)	٢٠٠٠	٧٥٠٠٠	٢٥٠٠٠
	خدمات تقييم الثغرات الأمنية (Vulnerability Assessment)	٢٠٠٠	٥٠٠٠٠	١٦٠٠٠
الخدمات الأمنية المدارة	خدمات مراقبة مركز العمليات الأمنية (SOC)	٢٠٠٠	١٢٠٠٠٠	٤٠٠٠٠
	خدمات الاستجابة للحوادث السيبرانية (Incident Response)	٢٠٠٠	٥٠٠٠٠	١٦٠٠٠
	خدمات تحليل الأدلة الرقمية (Digital Forensics)	٢٠٠٠	٥٠٠٠٠	١٦٠٠٠
خدمات الحلول المتكاملة والاستشارية والتدريب	خدمات الحلول المتكاملة والاستشارية	٢٠٠٠	١٥٠٠٠٠	٥٠٠٠٠
	خدمات التدريب	٢٠٠٠	٧٥٠٠٠	٢٥٠٠٠
خدمات تصنيف كوادر الأمن السيبراني		٢٠٠٠	٧٥٠٠٠	٢٥٠٠٠

مقابل إصدار/تجديد شهادة التسجيل (المستوى الثاني)

الخدمات		المقابل (جنيه مصري)		
		طلب الحصول على شهادة التسجيل	إصدار أو تجديد شهادة التسجيل	إصدار الشهادة المؤقتة
خدمات التقييم الأمني	اختبارات الاختراق (Penetration Testing)	١٠٠٠	٣٠,٠٠٠	١٠,٠٠٠
	خدمات الفريق الأحمر (Red teaming)	١٠٠٠	٢٠,٠٠٠	٧٠٠٠
	خدمات تقييم الثغرات الأمنية (Vulnerability Assessment)	١٠٠٠	١٥,٠٠٠	٥٠٠٠
الخدمات الأمنية المدارة	خدمات مراقبة مركز العمليات الأمنية (SOC)	١٠٠٠	٣٠,٠٠٠	١٠,٠٠٠
	خدمات الاستجابة للحوادث السيبرانية (Incident Response)	١٠٠٠	١٥,٠٠٠	٥٠٠٠
	خدمات تحليل الأدلة الرقمية (Digital Forensics)	١٠٠٠	١٥,٠٠٠	٥٠٠٠
خدمات الحلول المتكاملة والاستشارية والتدريب	خدمات الحلول المتكاملة والاستشارية	١٠٠٠	٤٠,٠٠٠	١٠,٠٠٠
	خدمات التدريب	١٠٠٠	٢٠,٠٠٠	٧٠٠٠
خدمات تصنيف كوادر الأمن السيبراني		١٠٠٠	١٥,٠٠٠	٥٠٠٠

سابعاً

متطلبات وإجراءات اعتماد الافراد

اعتماد الأفراد	المقابل (جنيه مصري)
طلب الحصول على شهادة الاعتماد	**١٠٠٠**
إصدار أو تجديد شهادة الاعتماد	**٤٠٠٠**

يتم تقديم طلب لاعتماد الأفراد العاملين بخدمات الأمن السيبراني لدى مقدمي خدمات الأمن السيبراني. كما يمكن للأفراد تقديم طلب للاعتماد، على أن يتضمن الطلب ما يلي:

١. اسم الشخص وجنسيته.
٢. بطاقة الرقم القومي أو رقم تصريح العمل أو رقم جواز السفر أو رقم الهوية الأجنبي.
٣. محل الاقامة (وإذا كان مختلفًا عن المذكور ببطاقة الرقم القومي) يتم توضيح عنوان للمراسلات.
٤. رقم الهاتف وعنوان البريد الإلكتروني.
٥. السيرة الذاتية متضمنة الخبرات الأكاديمية والمهنية.
٦. الشهادات والاعتمادات الفنية من الجهات المختلفة مع تحديد تلك الجهات وتاريخ الحصول على تلك الشهادات أو الاعتمادات ومدة صلاحيتها.
٧. مؤهلات مقدم الطلب وخبرته (إن وجدت) فيما يتعلق بخدمة الأمن السيبراني محل الاعتماد.
٨. صحيفة الحالة الجنائية مع تقديم ما يثبت التحري الأمني عن الأفراد المراد اعتمادهم
٩. اجتياز الإجراءات المتعلقة بالاستعلام الأمني وتقييم الحالة الصحية والائتمانية للمتقدم.
١٠. سداد مقابل إصدار شهادة الاعتماد طبقاً لجدول مقابل إصدار شهادة الاعتماد.
١١. شهادة تفيد بإتمام ٤٠ ساعة من التطوير المهني السنوي.
١٢. وثيقة (عدم الإفصاح عن اي بيانات للمستفيدين من الخدمات والحفاظ علي سرية المعلومات) والموافقة على ما يتبعها من شروط قانونية وجنائية.
١٣. أي بيانات أو إيضاحات يطلبها الجهاز في عملية التقييم.

ثامناً

إجراءات توفيق الأوضاع

يلتزم كل من يقوم بتقديم خدمات الأمن السيبراني لأي جهة مستفيدة داخل جمهورية مصر العربية عند صدور الإطار التنظيمي بتوفيق أوضاعهم خلال عام من تاريخ اعتماد الإطار وذلك طبقاً للإجراءات التالية:

١. يتم نشر الإطار التنظيمي الماثل على الموقع الرسمي للجهاز.

٢. يلتزم كل من يقوم بتقديم خدمات الأمن السيبراني خلال عام من تاريخ اعتماد الإطار ونشره بالتقدم للجهاز بطلب للتسجيل/للاعتماد لدى الجهاز وذلك مع تقديم المستندات الآتية:

- هيكل الشركة وموقفها المالي وقائمة المساهمين (في حالة الشركات).
- السيرة الذاتية متضمنة الخبرات الأكاديمية والمهنية (في حالة الأفراد).
- سابقة الأعمال والخبرات المحلية والدولية وقائمة بكافة العملاء الحاليين.
- الشهادات والاعتمادات الفنية من الجهات المختلفة مع تحديد تلك الجهات وتاريخ الحصول على تلك الشهادات أو الاعتمادات ومدة صلاحيتها.
- أي بيانات أو ايضاحات يطلبها الجهاز في عملية التقييم.

٣. يقوم الجهاز بدراسة الطلبات المقدمة خلال مدة ٩٠يوم من تاريخ تقديم الطلب للجهاز بشرط استيفاء كافة البيانات اللازمة لدراسة الطلبات، وفقاً للتالي:

- في حالة قبول الطلب، يتم إصدار شهادة التسجيل/الاعتماد مع التزام مقدم الطلب بتنفيذ كافة الالتزامات التي يحددها الجهاز.
- في حالة عدم قبول الطلب، يتم إخطار مقدم الطلب بحيثيات الرفض ويجوز إعادة تقديم الطلب خلال شهر بحد أقصى من تاريخ إخطار الرفض على أن يقوم الجهاز بالرد على الطلب المعاد تقديمه خلال مدة ٣٠ يوم من تاريخ تقديمه.

٤. بعد انقضاء عام من تاريخ اعتماد ونشر الإطار التنظيمي، وفي حالة عدم الحصول على شهادة التسجيل/الاعتماد من الجهاز، يعد ذلك مخالفاً لأحكام الإطار وللجهاز اتخاذ الإجراءات التنظيمية اللازمة في هذا الشأن.

ملحق (١)

خدمات الأمن السيبراني

أولاً: خدمات التقييم الأمني

١. اختبارات الاختراق (Penetration Testing)

يقصد بها تنفيذ لهجوم سيبراني مصرح به ومرخص على نظام أو شبكة وإجراء فحص شامل ودقيق وذلك لتحديد واختبار وكشف نقاط الضعف والتحقق من الثغرات الأمنية القابلة للاستغلال وذلك بهدف تقييم الوضع الأمني للنظام ورفع مستوي الأمان للتطبيقات والشبكات. وأنواع اختبارات الاختراق:

- **اختراق تطبيقات الويب (Web application penetration test)**

هو ممارسة لمحاكاة الهجمات على تطبيق يتم تشغليه على خادم ويب ((**web server**ويتم الوصول اليه من خلال متصفح الويب (**web browser**) بخلاف البرامج المعتمدة على الكمبيوتر والتي يتم تشغيلها داخليًا على نظام التشغيل (**OS**) للجهاز.

- **اختراق تطبيقات الهواتف المحمولة(Mobile application)**

اختبار أمني يتم إجرائه على التطبيقات التي تعمل على أنظمة التشغيل الخاصة بالهواتف المحمولة سواء كانت **IOS** أو**Android**

- **اختراق تطبيقات سطح المكتب(Desktop application)**

اختبار يستهدف التطبيقات التي تعمل بشكل مستقل في كمبيوتر مكتبي أو لاب توب على النقيض من "تطبيقات الويب"، والتي تتطلب تشغيل متصفح الويب(**web browser**)

- **اختراق البنية التحتية الخارجية(External Infrastructure)**

اختبار اختراق شبكة البنية التحتية للشبكة الخارجية (المواجهة للإنترنت) التي تنتمي إلى مؤسسة.

- **اختراق البنية التحتية الداخلية(Internal Infrastructure)**

اختبار اختراق البنية التحتية للشبكة الداخلية التي تنتمي إلى مؤسسة.

- **اختراق شبكات نقل الصوت عبر بروتوكول الانترنت(VoIP network) VoIP**

اختبار خاص لتحديد الثغرات التي قد تسمح باختراق شبكة VoIP أو إساءة استخدامها لإجراء مكالمات غير مصرح بها أو اعتراض المحادثات عبر شبكة المؤسسة.

- **اختراق الشبكات اللاسلكية(SSIDs profiles) Wi-Fi**

هو محاولة لتحديد نقاط الضعف الكامنة في عناصر التحكم في الأمان المستخدمة من قبل التقنيات اللاسلكية وبروتوكولات الأمان الضعيفة.

٢. خدمات الفريق الأحمر (Red teaming)

يقصـــد بها اختبار تنفيذ هجمات حقيقية الهدف منها اختراق الأنظمة أو البيانات الآمنة ويتم الاختبار دون علم أو تعاون من فريق أمن المؤسسة بهدف تقييم استجابة فريق أمن المؤسسة للتهديدات المختلفة.

٣. خدمات تقييم الثغرات الأمنية (Vulnerability Assessment)

يقصد بها خدمات لتقييم نقاط الضعف الأمنية في جميع أنظمة تكنولوجيا المعلومات وذلك بتقييم الأجهزة والأنظمة والشبكات والتطبيقات لنقاط الضعف الأمنية، حيث يتم تقييم ما إذا كان النظام عرضة لأي ثغرات أمنية عن طريق معرفة الخدمات التي تستخدم على الأجهزة ومعرفة إصدارات الخدمات عليها ونظام التشغيل ثم تحديد مستويات الخطورة لتلك الثغرات ومعالجتها.

- **شروط خاصة بمقدمي خدمات التقييم الأمني**

المستوى الأول	المستوى الثاني
توظيف ما لا يقل عن "٥" مقيمين في مجال الخدمة المقدمة من الشركة بحيث يكون: ● عدد ٢ من المقيمين حاصلين على شهادة دولية واحدة بحد أدنى "**Entry Level**" ● عدد ٢ من المقيمين حاصلين على شهادة دولية واحدة بحد أدنى "**Intermediate level** " ● عدد واحد مقيم حاصل على شهادة دولية واحدة بحد أدنى "**Advanced level**". يقوم الجهاز باعتماد الشهادات الدولية في هذا الصدد وفقاً للشهادات المحددة بالمرفق رقم (١).	توظيف ما لا يقل عن "٣" مقيمين في مجال الخدمة المقدمة من الشركة بحيث يكون: ● عدد ٢ من المقيمين حاصلين على شهادة دولية واحدة بحد أدنى "**Entry Level**" ● عدد ١ مقيم حاصل على شهادة دولية واحدة بحد أدنى " **Intermediate level**" يقوم الجهاز باعتماد الشهادات الدولية في هذا الصدد وفقاً للشهادات المحددة بالمرفق رقم (١).

ثانياً: الخدمات الأمنية المدارة

١. خدمات مركز مراقبة العمليات الأمنية (SOC)

تهدف الي اكتشاف التهديدات السيبرانية في مراحلها المبكرة والاستجابة لها ومعرفة كيفية حدوثها وتقديم التوصيات الشاملة في كيفية معالجتها واتخاذ الإجراءات اللازمة لاحتوائها، يجب أن يقوم مقدم خدمة الـــ **SOC** بالمراقبة على مدار الساعة لمنظومة المؤسسة ومراقبة البيانات لتحديد النشـاط المشـبوه، وتحديد المخاطر والتخفيف من حدتها قبل حدوث اختراق، ويعتبر الهدف الأسـاسـي لخدمات ال **SOC**هو التأكد من أن الأصـول الرقمية للمؤسـسـة آمنة ومحمية من الوصـول غير المصـرح به. مما يعني انها مسـؤولة عن حماية البنية التحتية في مكان العمل، في حالة حدوث اختراق، سيكون مقدم خدمات ال **SOC** على الخط الأمامي، ليعمل على مواجهة الهجوم، وفيما يلي وصفاً لأهم خدمات مراقبة مراكز العمليات الأمنية:

- المراقبة المستمرة واكتشاف التهديدات على مدار (٢٤/٧) (**Monitoring and Detection**)
- التحليل والتحقيق للتهديدات المختلف (**Threat Analysis and Investigation**)
- احتواء التهديدات السيبرانية (**Threat Containment**)

٢. خدمات الاستجابة للحوادث السيبرانية (Incident Response)

تهدف إلى مساعدة المؤسسات على التعامل مع التهديدات الأمنية بفعالية وسرعة وتقليل التأثيرات السلبية على عملياتهم وبياناتهم وذلك من خلال التعامل مع الحوادث الأمنية والسيبرانية بشكل فعال ومنهجي عند وقوعها. تتضمن هذه الخدمات استجابة سريعة ومنهجية للهجمات السيبرانية والأحداث الأمنية غير المرغوب فيها بهدف ضمان استمرارية العمل.

٣. خدمات تحليل الأدلة الرقمية (Digital Forensics)

الخدمات المستخدمة لجمع وتحليل البيانات الرقمية والإلكترونية بهدف استخلاص المعلومات والأدلة التي يمكن استخدامها في التحقيقات الجنائية أو الأمنية. يتم تطبيق تحليل الأدلة الرقمية على مجموعة متنوعة من الأمور، مثل التحقيق في جرائم القرصنة السيبرانية، واختراق الأنظمة، واسترداد البيانات المحذوفة، والتحقيق في حالات انتهاك البيانات.

- **شروط خاصة بمقدمي الخدمات الأمنية المدارة**

المستوى الأول	المستوى الثاني
توظيف ما لا يقل عن "٧" محللين في مجال الخدمة المقدمة بحيث يكون: ● عدد ٣ من المحللين حاصلين على شهادة دولية واحدة بحد أدنى "**Entry Level**" ● عدد ٣ من المحللين حاصلين على شهادة دولية واحدة بحد أدنى " **Intermediate level**" ● عدد واحد محلل حاصل على شهادة دولية واحدة بحد أدنى "**Advanced level**" ويقوم الجهاز باعتماد الشهادات الدولية في هذا الصدد وفقاً للشهادات المحددة بالمرفق رقم (١)	توظيف ما لا يقل عن "٥" محللين في مجال الخدمة المقدمة بحيث يكون: ● عدد ٣ من المحللين حاصلين على شهادة دولية واحدة بحد أدنى "**Entry Level**" ● عدد ٢ من المحللين حاصلين على شهادة دولية واحدة بحد أدنى " **Intermediate level**" ويقوم الجهاز باعتماد الشهادات الدولية في هذا الصدد وفقاً للشهادات المحددة بالمرفق رقم (١)

ثالثاً: خدمات الحلول المتكاملة والاستشارية والتدريب

خدمات الحلول المتكاملة والاستشارية: وهي التي تقدمها الشركات في مجال حلول الأمن السيبراني والمتضمنة تركيب أو توريد أو تشغيل أنظمة أو أجهزة من شركات الأمن السيبراني المتخصصة العالمية والمقدمة للجهات المستفيدة من الفئة الأولى والثانية.

خدمات التدريب: وهي الخدمات التي تتضمن تقديم برامج تعليمية وتدريبية في مجالات الأمن السيبراني المختلفة لبناء القدرات ورفع مستوى المعرفة لدى الشركات والافراد بسياسات وضوابط الأمن السيبراني وتختص في تدريب الافراد للحصول على رخص شهادات المهارات السيبرانية.

- **شروط خاصة بمقدمي خدمات الحلول المتكاملة والاستشارية (المستوى الأول والثاني)**

استيفاء العاملين لأحد المتطلبات الآتية :

١. حديث التخرج من أحد برامج الأمن السيبراني المعتمدة من كليات الهندسة أو علوم الحاسب تخصص (اتصالات – حاسب – أمن سيبراني).
٢. خريج (٣ سنوات خبرة) من أحد كليات الهندسة أو علوم الحاسب تخصص (اتصالات – حاسب –امن سيبراني).
٣. الحصول على أحد دورات الأمن السيبراني المؤهلة بالمعاهد التابعة لوزارة الاتصالات وتكنولوجيا المعلومات.

- **شروط خاصة بمقدمي خدمات التدريب في مجال الأمن السيبراني**

المستوى الأول	المستوى الثاني
توظيف ما لا يقل عن "٥" مقيمين في مجال الخدمة المقدمة من الشركة بحيث يكون: ● عدد ٣ من المدربين حاصلين على شهادة دولية واحدة بحد أدنى "**Intermediate level** " ● عدد ٢ من المدربين حاصلين على شهادة دولية واحدة بحد أدنى "**Advanced level**". يقوم الجهاز باعتماد الشهادات الدولية في هذا الصدد وفقاً للشهادات المحددة بالمرفق رقم (١)	توظيف ما لا يقل عن "٣" مقيمين في مجال الخدمة المقدمة من الشركة بحيث يكون: ● عدد ٢ من المدربين حاصلين على شهادة دولية واحدة بحد أدنى "**Intermediate level** " ● عدد واحد مدرب حاصل على شهادة دولية واحدة بحد أدنى "**Advanced level**". يقوم الجهاز باعتماد الشهادات الدولية في هذا الصدد وفقاً للشهادات المحددة بالمرفق رقم (١)

رابعاً: خدمات التقييم والتصنيف لكوادر الأمن السيبراني

يقصد بها خدمات تصنيف وتقييم معارف ومهارات وقدرات العاملين في مجال الأمن السيبراني وتضمن هذه الخدمات أن الافراد مؤهلين للوظائف المطلوبة منهم. يهدف عمل هذه الشركات إلى تقديم تقييم شامل ودقيق المهارات الفنية أو الشخصية للأفراد العاملين في مجال الأمن السيبراني، سواء كانوا موظفين في الشركات أو مستقلين.

- **شروط خاصة بمقدمي خدمات التقييم والتصنيف لكوادر الأمن السيبراني التقييم والتصنيف لكوادر الأمن السيبرانية (المستوى الأول والثاني)**

توظيف ما لا يقل عن "٣" مقيمين في مجال الخدمة المقدمة من الشركة بحيث يكون أحد المقيمين على الأقل حاصل على شهادة دولية واحدة "**Advanced Level**" وان يكون باقي المقيمين حاصلين على شهادات بحد أدني " **Intermediate Level**". ويشترط لكي يتم تصنيف المتقدم إلى أحد المستويات (**Advanced – intermediate – entry**) أن يكون المقيم حاصل على شهادة من نفس المستوي أو اعلي.

ويقوم الجهاز القومي باعتماد الشهادات الدولية في هذا الصدد وفقاً للشهادات المحددة بالمرفق رقم (١).

مرفق (١)

الشهادات الدولية

أ-الشهادات المعتمدة للعمل كـ "مقيم أمني"

اشتراطات خاصة او ملاحظات	الشهادة	الجهة المصدرة
Intermediate level	Offensive Security Wireless Professional (OSWP)	Offensive Security
Advanced level	Offensive Security Web Expert (OSWE)	
Advanced level	Offensive Security Exploitation Expert (OSEE)	
Intermediate level	Offensive Security Certified Professional (OSCP)	
Intermediate level	Offensive Security Exp. Penetration Tester (OSEP)	
Intermediate level	Offensive Security Exploit Developer (OSED)	
Advanced level	Offensive Security Exploitation Expert (OSEE)	
Advanced level	Offensive Security Certified Expert (OSCE)	
Advanced level	Licensed Penetration Testing (LPT)	International Council of E-Commerce Consultants
Intermediate level	ECSA – EC Council Certified Security Analyst	
Advanced level	Certified Penetration Testing Professional (CPENT)	
Intermediate level	Certified Ethical Hacker (C|EH)	
Advanced level	Licensed Penetration Tester (LPT)	
Advanced level	(C|EH) Master	
Intermediate level	Infosec Institute Certified Penetration Tester (CPT)	Infosec Institute
Intermediate level	Certified Red Team Operations Professional (CRTOP)	
Intermediate level	Certified Mobile and Web Application Pen. Tester (CMWAPT)	
Advanced level	Certified Expert Penetration Tester (CEPT)	
Entry Level	GIAC Penetration Tester (GPEN)	GIAC
Intermediate level	GIAC Web Application Penetration Tester (GWAPT)	
Advanced Level	Security Leadership Certification (GSLC)	
Advanced Level	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking (GXPN)	
Entry level	CompTIA Security+	CompTIA
Intermediate Level	CompTIA Pen Test+	

ب- الشهادات المعتمدة للعمل بتقديم خدمات مراقبة مركز العمليات الأمنية.

اشتراطات خاصة او ملاحظات	الشهادة	الجهة المصدرة
Intermediate Level	Certified SOC Analyst (CSA)	EC-Council University
Intermediate Level	CompTIA Cybersecurity Analyst (CYSA+)	CompTIA
Advanced Level	CompTIA Advanced Security Practitioner (CASP+)	
Entry Level	GIAC Information Security Fundamentals (GISF)	GIAC Certifications
Entry Level	GIAC Security Essentials (GSEC)	
Intermediate Level	GIAC Certified Incident Handler (GCIH)	
Intermediate Level	GIAC Security Operations Certified (GSOC)	
Intermediate Level	GIAC Certified Intrusion Analyst (GCIA)	
Intermediate Level	GIAC Continuous Monitoring Certification (GMON)	
Advanced Level	GIAC Certified Detection Analyst (GCDA)	
Advanced Level	GIAC Defensible Security Architecture (GDSA)	
Intermediate Level	Certified in Risk and Information Systems Control (CRISC)	ISACA

ت- الشهادات المعتمدة للعمل بتقديم خدمات الاستجابة للحوادث السيبرانية.

اشتراطات خاصة او ملاحظات	الشهادة	الجهة المصدرة
Intermediate Level	Certified Incident Handler (ECIH)	EC-Council University
Intermediate Level	Certified Incident Handler (GCIH)	
Entry Level	GIAC Security Essentials (GSEC)	GIAC Certifications
Intermediate Level	GIAC Certified Forensic Examiner (GCFE)	
Advanced Level	GIAC Certified Forensic Analyst (GCFA)	
Advanced Level	GIAC Cloud Forensics Responder (GCFR)	
Advanced Level	GIAC Network Forensic Analyst (GNFA)	

ث- الشهادات المعتمدة للعمل بتقديم خدمات تحليل الأدلة الرقمية.

اشتراطات خاصة او ملاحظات	الشهادة	الجهة المصدرة
Intermediate Level	Computer Hacking Forensic Investigator (CHFI)	EC-Council University
Intermediate Level	Certified Threat Intelligence Analyst (CTIA)	
Entry Level	CompTIA Security+	CompTIA
Intermediate Level	GIAC Security Operations Certified (GSOC)	
Intermediate Level	Certified Forensic Examiner (GCFE)	
Entry Level	GIAC Information Security Fundamentals (GISF)	GIAC Certifications
Entry Level	GIAC Security Essentials (GSEC)	
Entry Level	GIAC Battlefield Forensics and Acquisition (GBFA)	
Intermediate Level	GIAC Certified Forensic Examiner (GCFE)	
Advanced Level	GIAC Certified Forensic Analyst (GCFA)	

Advanced Level	GIAC Cloud Forensics Responder (GCFR)	
Advanced Level	GIAC Advanced Smartphone Forensics (GASF)	
Advanced Level	GIAC iOS and macOS Examiner (GIME)	

ج- الشهادات الواجب توافرها للأفراد بالشركات القائمة بالتدريب الأمني

اشتراطات خاصة أو ملاحظات	الشهادة	الجهة المصدرة
Advanced Level	(ISC)2 Certified Information Systems Security Professional (CISSP);	(ISC)2
Advanced Level	(ISC)2 Certified Cloud Security Professional (CCSP)	
Advanced Level	Certified Penetration Testing Professional (CPENT)	EC-Council University
Intermediate Level	EC-Council CEH (Practical);	
Advanced Level	ISACA Certified Information Security Manager (CISM)	ISACA
Intermediate Level	Offensive Security Certified Professional (OSCP)	Offensive Security
Advanced Level	Offensive Security Web Expert (OSWE)	
Advanced Level	Offensive Security Certified Expert (OSCE)	
Advanced Level	GIAC Certified Forensic Analyst (GCFA)	GIAC Certifications
Intermediate Level	GIAC Certified Forensic Examiner (GCFE)	
Intermediate Level	GIAC Security Operations Certified (GSOC)	
Advanced Level	GIAC Advanced Smartphone Forensics (GASF)	
Advanced Level	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking (GXPN)	
Advanced Level	Law of Data Security and Investigations (GLEG)	
Intermediate Level	Tenable Certified Nessus Auditor (TCNA)	Vendor specific
Intermediate Level	Tenable Certified Passive Vulnerability Scanner Auditor (TCPA)	

مرفق (٢)

قطاعات البنية التحتية الحرجة

القطاع	أمثلة
قطاع الخدمات الحكومية	بوابة ومواقع الحكومة الإلكترونية، ومواقع الجهات والمؤسسات الحكومية، وقواعد البيانات والمعلومات القومية وأهمها قاعدة الحكومة الرقمية وبيانات الرقم القومي والشبكات والمواقع المتصلة بها وغيرها.
قطاع النقل والمواصلات	وزارة النقل وجميع الهيئات التابعة مثل النقل البري والبحري والجوي والنيلي، ويضم كافة نظم ومراكز وشبكات التحكم في القطارات والمترو، وشبكات المرور، ونظم التحكم في الملاحة الجوية والبحرية.
قطاع الطاقة	وزارة الكهرباء والبترول وجميع الهيئات التابعة لهما بالإضافة إلى نظم وشبكات ومحطات التحكم في إنتاج وتوزيع الكهرباء والبترول والغاز، ومحطات السد العالي، ومحطات الطاقة النووية، وغيرها.
قطاع الاتصالات وتكنولوجيا المعلومات	وزارة الاتصالات وتكنولوجيا المعلومات والجهات التابعة لها بما يشمل شبكات الاتصالات السلكية واللاسلكية، والكوابل البحرية والأرضية، وأبراج الاتصالات، والأقمار الصناعية للاتصالات، ومراكز التحكم في الاتصالات، وجميع شركات الاتصالات والإنترنت المرخص لها العاملة في القطاع العام والقطاع الخاص.
قطاع الصحة وخدمات الإسعاف العاجل	وزارة الصحة والجهات التابعة لها بما فيها من شبكات الإغاثة والإسعاف، وبنوك الدم، ونظم وشبكات المستشفيات، وشبكات ومواقع تقديم الرعاية الصحية.
قطاع الإعلام والثقافة	وزارة الأعلام والجهات التابعة لها ويشمل شبكات ونظم ومواقع الخدمات الإعلامية والبث.
قطاع الخدمات المالية	وزارة المالية والجهات التابعة لها وتشمل شبكات ومواقع البنوك، وشبكات ومواقع تقديم المعاملات المصرفية، وشبكات الدفع الإلكتروني، وشبكات ومواقع البورصة، وشركات تداول الأوراق المالية، وشبكات الخدمات المالية البريدية.
وزارة التجارة والصناعة	وزارة التجارة والصناعة والجهات التابعة لها وتشمل جميع الشبكات والخدمات المقدمة.
قطاع التموين	وزارة التموين والجهات التابعة وتشمل أنظمة هيئة السلع الاستراتيجية وقطاع التجزئة.
قطاع الصناعات الكيماوية	مصانع الكيماويات والأسمدة والبتروكيماويات وما يماثلها.
قطاع السياحة	وزارة السياحة والجهات التابعة وتشمل القرى والفنادق والنقل السياحي وما يماثلها.

وذلك بالإضافة الي المواقع الرسمية للدولة والقطاعات ذات التأثير علي النشاط الاقتصادي مثل الاستثمار والسياحة والتجارة والصناعة والزراعة والري والتعليم بمختلف مستوياته ومحطات مياه الشرب والصرف الصحي والموارد المائية وغيرها من مرافق المعلومات والاتصالات التي قد تؤثر على الأمن القومي أو الاقتصاد القومي والمصلحة العامة وما في حكمها."