تعليمات ترخيص خدمة الاستجابة لحوادث الأمن السيبراني لسنة ٢٠٢٦

صادرة بمقتضى المادة (١٥) من نظام ترخيص مقدمي خدمات الأمن السيبراني رقم (٧٦) لسنة ٢٠٢٤

المادة ١-تسمى هذه التعليمات (تعليمات ترخيص خدمة الاستجابة لحوادث الأمن السيبراني لسنة ٢٠٢٦) ويعمل بها من تاريخ نشرها في الجريدة الرسمية.

المادة٢- أ- يكون للكلمات والعبارات التالية حيثما وردت في هذه التعليمات المعاني المخصصة لها أدناه ما لم تدل القرينة على غير ذلك:

القانون	:	قانون الأمن السيبراني.
النظام	:	نظام ترخيص مقدمي خدمات الأمن السيبراني .
المركز	:	المركز الوطني للأمن السيبراني.
خدمة الاستجابة لحوادث الأمن السيبراني	:	العمليات والإجراءات التي يتبعها فريق الاستجابة لاكتشاف الهجمات وحوادث الأمن السيبراني والتعامل معها وتحديد نطاقها واحتوائها والحد من الأضرار الناتجة عنها ومعالجتها.
الاستجابة	:	مجموعة الإجراءات والتدابير التقنية والأمنية والقانونية التي تتخذها الجهة المعنية عند وقوع حادث الأمن السيبراني.
حادث الأمن السيبراني	:	الفعل أو الهجوم الذي يشكل خطراً على البيانات أو المعلومات أو نظم المعلومات أو الشبكة المعلوماتية أو البنى التحتية المرتبطة بها ويتطلب استجابة لإيقافه أو للتخفيف من العواقب أو الآثار المترتبة عليه.
محلل الاستجابة	:	الشخص المسؤول عن فهم طبيعة حادث الأمن السيبراني وتحديد نطاقه، وتحليل أثره على الجهة وتحديد السبب المؤدي لوقوعه.
فريق الاستجابة	:	الخبراء المعنيون بتقديم خدمة الاستجابة لحوادث الأمن السيبراني لدى مقدم الخدمة.
الدليل الرقمي	:	أي بيانات أو معلومات يتم إنشاؤها أو تخزينها أو معالجتها أو نقلها بواسطة أجهزة أو أنظمة إلكترونية أو رقمية، ويمكن استخدامها لإثبات واقعة مادية أو فعل في إطار التحقيقات أو الإجراءات القضائية، بما في ذلك الملفات الإلكترونية، والرسائل الرقمية، وسجلات الدخول، والصور، والتسجيلات، والبيانات الموقعة إلكترونياً وسجلات الشبكات، شريطة أن تكون هذه البيانات قد تم جمعها وتحليلها بطرق تضمن سلامتها ومصداقيتها، وفقاً للمعايير الفنية والقانونية المعتمدة.

ب- تعتمد التعاريف الواردة في النظام حيثما ورد النص عليها في هذه التعليمات ما لم تدل القرينة على غير ذلك.

المادة ٣ -على مقدم طلب الحصول على ترخيص خدمة الاستجابة لحوادث الأمن السيبراني الالتزام بما يلي:-

أ- شروط ومتطلبات الترخيص المنصوص عليها في النظام.

ب- تقديم طلب الترخيص ورقياً أو إلكترونياً إلى المركز على النموذج المعتمد لهذه الغاية، مرفقاً به ما يلي: -

١. الشهادات والوثائق التي تثبت تحقق شروط ومتطلبات الترخيص المنصوص عليها في النظام.
٢. الخبرات السابقة والمشاريع المنفذة من قبل الجهة طالبة الترخيص داخل المملكة وخارجها في مجال خدمة الاستجابة لحوادث الأمن السيبراني.
٣. وصف فني لآلية تقديم خدمة الاستجابة لحوادث الأمن السيبراني وإجراءات العمل والأنظمة والتقنيات التي سيتم استخدامها لهذه الغاية في حال لم تكن لدى الجهة طالبة الترخيص خبرة سابقة.
٤. وثيقة تتضمن أسماء أعضاء فريق الاستجابة مرفقة بها سيرهم الذاتية وصور عن الشهادات المصدقة والوثائق التي تثبت خبراتهم في تقديم خدمة الاستجابة لحوادث الأمن السيبراني.
٥. شهادات اعتماد سارية المفعول صادرة عن المركز في حال سبق الحصول عليها تخول فريق الاستجابة تقديم الخدمة.
٦. قائمة بأدوات وبرمجيات الاستجابة التي سيستخدمها مقدم الخدمة عند تقديم الخدمة، ومميزاتها، ومكان الاستضافة، على أن تكون هذه الأدوات والبرمجيات من مصدر موثوق به.
٧. عقد العمل أو الاتفاقية الموقعة مع أعضاء فريق الاستجابة.
٨. أي شهادات اعتماد دولية سارية المفعول في مجال تقديم خدمة الاستجابة لحوادث الأمن السيبراني حصل عليها مقدم طلب الترخيص.
٩. وصل مقبوضات بدل دراسة طلب تقديم خدمة الاستجابة لحوادث الأمن السيبراني.
١٠. أي معلومات أو مستندات أو وثائق أخرى يراها المركز ضرورية لإصدار قراره بشأن طلب الترخيص.

ج- للمركز إجراء الكشف على مقر مقدم طلب الترخيص في العنوان المحدد في الطلب للتحقق من المعلومات المقدمة وتقييم إمكاناته وقدراته.

المادة ٤ - مع مراعاة الأحكام المنصوص عليها في هذه التعليمات، على مقدم الخدمة عند تقديمه خدمة الاستجابة لحوادث الأمن السيبراني، الالتزام بما يلي: -

أ-الامتثال للتشريعات النافذة والأطر التنظيمية والمعايير والضوابط والسياسات الصادرة عن المركز بما فيها تلك المتعلقة بمنتجات الأمن السيبراني.

ب-إعداد خطة لإدارة الاستجابة تتوافق في خطواتها وتفاصيلها مع ما يلي:-

١- الإطار الوطني للأمن السيبراني.

٢- المعايير العالمية القياسية في الاستجابة لحوادث الأمن السيبراني كالمعيار (ISO/IEC٢٧٠٣٥) الصادر عن المنظمة الدولية للمعايير أو دليل الاستجابة لحوادث أمن الحاسوب الصادر عن المعهد الوطني للمعايير والتكنولوجيا (NIST SP ٨٠٠-٦١)
٣- أي سياسات أو معايير أو أدلة إرشادية يعتمدها المركز لاحقاً.

ج-تحديد الأهداف والمنهجية وهيكلية الفريق وإعداد خطة الاتصال ومؤشرات قياس أداء الخدمة حداً أدنى وتضمينها في خطة الاستجابة.
د-وضع إجراءات تشغيل قياسية لتحديد العمليات الفنية، والتقنيات، وقوائم المراجعة والنماذج المحددة التي سيستخدمها فريق الاستجابة بحيث تغطي الأنشطة والمهام التفصيلية اللازمة قبل الاستجابة وخلالها وبعدها، وعلى النحو التالي: -
١- الاستعداد والتحضير لعمليات الاستجابة.
٢- الكشف عن الحوادث السيبرانية وتحليلها.
٣- احتواء الحوادث السيبرانية والحد من أضرارها.
٤- إزالة الأسباب التي أدت إلى وقوع حادث الأمن السيبراني.
٥- التعافي من الحوادث السيبرانية واستعادة سير العمل الطبيعي.
٦- الإجراءات المتبعة بعد الحادث والدروس المستفادة.
هـ- تنفيذ اختبارات لإجراءات التشغيل القياسية للتحقق من دقتها وفاعليتها وكفاءتها.
و-إجراء مراجعات دورية مرة واحدة على الأقل سنويا على إجراءات التشغيل القياسية وتطبيق أي تحسينات لازمة عليها.
ز-تزويد فريق الاستجابة بالنسخة المعتمدة من إجراءات التشغيل القياسية، والتأكد من فهم أعضائه لمهامهم وقدرتهم على القيام بها.

المادة ٥- يُشترط في الأدوات والبرمجيات والأجهزة المستخدمة لتقديم خدمة الاستجابة لحوادث الأمن السيبراني ما يلي:-
أ- توافر الخصائص الأمنية اللازمة بما في ذلك تخزين البيانات والاحتفاظ بها بشكل آمن، والتحكم في النسخ الاحتياطي واستعادة البيانات، والمحافظة على سلامتها أثناء جمعها وتحليلها، وتوفير السجلات الملائمة، وضمان التحكم في الوصول والتحقق من الهوية والصلاحيات.
ب-القدرة على أداء مجموعة متنوعة من المهام، بما في ذلك نسخ الملفات والأقراص الصلبة، ونسخ ذاكرة نظام التشغيل، وتشفير الملفات والأقراص الصلبة والتحقق منها لضمان سلامتها.
ج-القدرة على استرجاع الملفات المحذوفة من أنظمة التشغيل واستخلاص البيانات الوصفية من الملفات، وتحليل سجلات الحوادث، وإعادة بناء البيانات مثل فك التشفير البسيط باستخدام أساليب محاولة اختراق نظام الأمان بتجربة كلمات مرور سهلة التخمين.

د- القدرة على تحليل البرمجيات الخبيثة في بيئة محمية ومراقبة، وتوفير معدات محمولة وقابلة للنقل إلى موقع الحادث.

المادة ٦ - أ-يشترط أن تتوفر في رئيس فريق الاستجابة المؤهلات والخبرات التالية: -

١- الشهادة الجامعية الأولى كحد أدنى في تكنولوجيا المعلومات أو أي تخصص ذي علاقة.

٢- خبرة عملية في مجال الأمن السيبراني أو أمن المعلومات لا تقل عن (٥) خمس سنوات منها (٣) ثلاث سنوات في مجال الاستجابة لحوادث الأمن السيبراني.

٣-شهادة مهنية واحدة كحد أدنى من الشهادات المهنية المعتمدة لدى المركز والمنشورة على الموقع الإلكتروني الخاص به .

ب-يشترط في أعضاء فريق الاستجابة ما يلي:-

١- أن يكون أعضاء الفريق من ذوي الاختصاص والكفاءة، على أن يضم الفريق (٣) ثلاثة محللين استجابة، يتولى أحدهم رئاسة الفريق.

٢- الحصول على الشهادة الجامعية الأولى أو شهادة الدبلوم المتوسط كحد أدنى من جامعة أو مؤسسة أكاديمية معترف بها.

٣- أن تكون لديهم خبرة عملية في مجال الأمن السيبراني أو أمن المعلومات لا تقل عن (٣) ثلاث سنوات منها سنة واحدة في مجال الاستجابة لحوادث الأمن السيبراني.

٤- شهادة مهنية واحدة كحد أدنى من الشهادات المهنية المعتمدة لدى المركز والمنشورة على الموقع الإلكتروني الخاص به.

ج- يلتزم مقدم الخدمة بتصميم وتنفيذ برنامج تدريبي لتطوير مهارات فريق الاستجابة بشكل مستمر، وتزويد المركز بما يثبت ذلك من خلال التقارير السنوية التي يقدمها للمركز.

المادة ٧- يلتزم مقدم الخدمة بما يلي: -

أ- توقيع اتفاقية عدم الإفصاح عن المعلومات للحفاظ على سرية المعلومات والبيانات التي يتم الاطلاع عليها، وعدم إفشائها أو مشاركتها مع أي طرف آخر أو نقلها خارج المملكة ما لم تنص التشريعات النافذة على غير ذلك.

ب- تزويد المركز بتقارير سنوية إحصائية تتضمن قائمة بخدمات الاستجابة التي نفذها شاملاً المعلومات عن الجهات المستفيدة من الخدمة، والخدمات المقدمة لهم وحفظ هذه التقارير بشكل آمن وضمان حماية الوصول إليها.

ج- عدم التعاقد من الباطن لتقديم خدمة الاستجابة إلا مع جهة مرخصة وفق الأصول من المركز.

د- الربط والتكامل مع أنظمة المركز ومنصاته بهدف أتمتة الإجراءات.

هـ- التعاون الكامل مع المركز خلال عمليات التدقيق التي يقوم بها ،وتزويد المركز بأي معلومات أو وثائق يراها ضرورية.

المادة ٨ -مع مراعاة أحكام هذه التعليمات، على مقدم الخدمة بعد تقديم خدمة الاستجابة، الالتزام بما يلي: -

أ- التحقق من الحادث المشتبه به، وجمع المعلومات اللازمة للتأكد من وقوعه.

ب- تصنيف الحادث وفق تعليمات تصنيف الحوادث الصادرة عن المجلس، وتحديد مستوى خطورته واتخاذ إجراءات الاستجابة المناسبة والتحقيق في أسباب وقوعه.
ج- اتخاذ جميع التدابير والإجراءات اللازمة لاحتواء حادث الأمن السيبراني ومعالجته بشكل فعّال، بما فيها الاستجابة السريعة، وجمع الأدلة الرقمية وتحليلها.
د- توثيق كافة تفاصيل حادث الأمن السيبراني، بما في ذلك، مدة الحادث، وأسبابه ونوعه، ومستوى خطورته، وتقييم أثره على متلقي الخدمة وعلى أي جهة متضررة.
هـ- توثيق عملية الاستجابة توثيقا كاملا، بما في ذلك القرارات المتخذة، والإجراءات التقنية والإدارية، وعمليات التقييم، والتحقق من الحوادث، والأدوات المستخدمة والأدلة التي تم جمعها.
و- الفصل بين بيانات متلقيّ الخدمة على مستوى قواعد البيانات، للحفاظ على الخصوصية والسرية.
ز-أن يكون جمع بيانات متلقي الخدمة ومعالجتها لأغراض محددة وصريحة تتعلق بتقديم الخدمة فقط.
ح-إعلام متلقي الخدمة بأي مشاهدات أو ثغرات أمنية قد تؤثر على سلامته أو سمعته خلال فترة تقديم الخدمة.
ط-تقديم تقرير تحليلي شامل لمتلقي الخدمة يتضمن ملخصاً للحادث، وتفاصيل عملية الاستجابة وملخصا لتقرير التحليل، وشرحا متكاملا للتسلسل الزمني للأحداث، إضافة إلى التدابير التي قد تتطلب متابعة على أن يتم تحديد مجالات التحسين وتقديم التوصيات المناسبة لتعزيز الأداء.

المادة ٩ - يلتزم مقدم خدمة الاستجابة لحوادث الأمن السيبراني بإبلاغ المركز عن أي مما يلي: -
أ- فقدان أي شرط من شروط أو متطلبات الترخيص المنصوص عليها في النظام.
ب- أي تغيير يطرأ على فريق الاستجابة، ويحظر على أي عضو جديد في الفريق تقديم الخدمة إلا بعد الحصول على شهادة من المركز تخوله ذلك، وتبقى الشهادة مرتبطة بالعضو، ولا تتأثر حال انتقاله من أحد مقدمي خدمة الاستجابة لحوادث الأمن السيبراني إلى آخر.
ج-أي تغيير يؤثر على قدرة وكفاءة مقدم الخدمة على تقديمها.
د- الحصول على معلومات أثناء تنفيذ الخدمة تشير إلى قيام متلقي الخدمة بارتكاب مخالفة للقانون والأنظمة والتعليمات الصادرة بمقتضاه.

المادة ١٠- يلتزم مقدم خدمة الاستجابة لحوادث الأمن السيبراني بتزويد المركز بشكل فوري بالمعلومات المبينة أدناه في حال كان تصنيف حادث الأمن السيبراني خطيراً أو شديد الخطورة، أو كان متلقي الخدمة جهة حكومية أو من قطاعات البنى التحتية الحرجة: -
أ- معلومات مقدم الخدمة.
ب- معلومات متلقي الخدمة المستهدف.
ج- الأصول المعلوماتية المستهدفة في حادث الأمن السيبراني والأدلة الرقمية التي تم جمعها.

د- مؤشرات الاختراق مثل حركة بيانات مشبوهة على الشبكة أو مؤشرات لبرمجيات أو فيروسات خبيثة أو محاولات فاشلة.

هـ - تاريخ ووقت وقوع حادث الأمن السيبراني.

المادة ١١-يحتفظ مقدم الخدمة بالمعلومات المتعلقة بخدمة الاستجابة لمدة لا تقل عن (٣) ثلاث سنوات من تاريخ الانتهاء من تقديم الخدمة على أن تتضمن ما يلي:-

أ- أسماء ومعلومات فريق الاستجابة، الذين شاركوا في تقديم كل خدمة استجابة.

ب- اسم ومعلومات متلقي الخدمة وتاريخ تقديم الخدمة ومدتها.

ج- التقنيات والأدوات المستخدمة.

د- أي معلومات أخرى يحددها المركز.

المادة ١٢- أ- على متلقي الخدمة، الالتزام بما يلي: -

١- التعاقد مع مقدم خدمة مُرخص وفقاً لأحكام النظام والتعليمات الصادرة بمقتضاه.

٢- التأكد من حصول فريق الاستجابة على شهادات مصدقة من المركز.

٣- التحقق من قيام مقدم الخدمة باتخاذ الإجراءات اللازمة للحفاظ على أمن معلوماته وبياناته باعتبار متلقي الخدمة المسؤول الأول عن حمايتها.

٤- تزويد مقدم الخدمة بالمعلومات والمتطلبات التي يحتاجها لتقديم الخدمة كالمخططات الفنية ونقاط الاتصال والمنافذ من الشبكة وإليها والحوادث السابقة وغيرها من المعلومات التي يتفق عليها الطرفان.

٥- إبلاغ المركز عن أي إخلال من قبل مقدم الخدمة بأي من المتطلبات المنصوص عليها في هذه التعليمات.

ب- لمتلقي الخدمة استشارة المركز فنياً قبل التوقيع على اتفاقية خدمة مع أيٍ من مقدمي خدمة الاستجابة لحوادث الأمن السيبراني المُرخصين.

المادة ١٣ - لغايات تنفيذ أحكام هذه التعليمات، يتولى المركز القيام بما يلي: -

أ-إجراء التدقيق السنوي على مقدمي الخدمة المُرخصين للتحقق من امتثالهم لمتطلبات وشروط الترخيص ومعايير الخدمة.

ب- نشر وتحديث سجل عام بمقدمي الخدمة المرخصين على مواقعه الإلكترونية ومنصاته الرقمية، على أن يتضمن أسماء مقدمي الخدمة وأرقام تراخيصهم وحالة الترخيص (فعّال، أو موقوف، أو ملغى) وخبراتهم ومعلومات التواصل الخاصة بهم .

ج-توثيق أي إجراءات تأديبية أو عقوبات يتم اتخاذها بحق مقدم الخدمة المرخص في السجل العام.

المادة ١٤- لرئيس المركز وبناء على تنسيب المديرية المعنية بالترخيص، إيقاف ترخيص مقدم الخدمة أو تعديله أو إلغاؤه قبل انتهاء مدته أو عدم تجديده في أي من الحالات التالية: -

أ-إذا أفشى أي وثائق أو معلومات أو بيانات سرية اطلع عليها بحكم عمله أو حصل عليها من متلقي الخدمة ، أو إذا ثبت عدم صحتها.

ب-إذا ارتكب أي مخالفة لأحكام القانون أو النظام أو هذه التعليمات ولم يعمل على إزالة المخالفة وأسبابها خلال مدة لا تزيد على (٦٠) ستين يوماً من تاريخ تبلغه بذلك خطياً أو الكترونياً.

ج-إذا ارتكب ثلاث مخالفات خلال السنة تبدأ من تاريخ ضبط أول مخالفة.

د-إذا فقد أي شرط من شروط الترخيص ولم يقم بتصويب أوضاعه خلال المدة المحددة في الفقرة (ب) من هذه المادة.

هـ-بناء على طلب مقدم الخدمة.

و-إذا ثبت للمركز عدم التزام مقدم الخدمة بمعايير تقديم خدمة الاستجابة لحوادث الأمن السيبراني المعمول بها، وذلك بناء على شكوى من متلقي الخدمة.

ز-إذا صدر بحقه حكم قضائي قطعي يقضي بإيقاف ترخيص مقدم الخدمة أو تعديله أو إلغائه .

ح-إذا اقتضت المصلحة العامة ذلك.

المادة ١٥- أ- تكون مدة الترخيص لخدمة الاستجابة لحوادث الأمن السيبراني ثلاث سنوات تبدأ من تاريخ إصدار الترخيص، وتجدد لمدة مماثلة وفقاً لأحكام النظام.

ب-يحظر على المرخص له الاستمرار في تقديم خدمته في حال عدم تجديد الترخيص.

المادة ١٦- كل من يخالف أحكام هذه التعليمات تطبق عليه أحكام المادة (١٦) من القانون وتعليمات تحديد معايير مخالفات أحكام قانون الأمن السيبراني وضوابطها والإجراءات المستحقة عليها.

المجلس الوطني للأمن السيبراني