تعليمات ترخيص خدمة الأمن السيبراني

المُدارة 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 الأمن السيبراني المُدارة لسنة ٢٠٢٦) ويعمل بها من تاريخ نشرها في الجريدة الرسمية.

المادة ٢-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 الأمن السيبراني المُدارة : الإجراءات الفنية والإدارية والتقنيات والأدوات التي تتضمن مراقبة الأصول التقنية وتحليلها وفحصها لمتلقي الخدمة والتعامل مع الحوادث والهجمات السيبرانية، وتشكل خط الدفاع الأول على مدار الساعة لحماية متلقي الخدمة من التهديدات السيبرانية المحتملة وتعزيز أمنها السيبراني.

فريق مركز العمليات : مجموعة من الخبراء المعتمدين لدى مقدم الخدمة لتقديم خدمة الأمن السيبراني المُدارة.

الاستجابة : مجموعة من الإجراءات التقنية والأمنية والتنظيمية والقانونية التي تتخذ عند وقوع حادث أمن سيبراني.

أصول المعلومات : جميع الموارد التي تحتوي على معلومات ذات قيمة للجهة بغض النظر عن شكلها أو وسيلة تخزينها أو نقلها بما في ذلك المعلومات المكتوبة والمطبوعة والإلكترونية، والأصول الرقمية التي تم إنشاؤها أو تخزينها أو معالجتها باستخدام أنظمة رقمية ويمكن الوصول إليها عبر شبكة الإنترنت أو الشبكات.

التهديد : أي حدث أو فعل أو حالة قد تؤدي إلى أضرار وتأثيرات وعواقب أمنية غير مرغوبة بأصول المعلومات .

المسوحات الأمنية : عمليات فحص للأصول الرقمية بقصد البحث عن ثغرات أمنية محتملة.

الاستخبارات السيبرانية : عملية منهجية ودورية يتم من خلالها رصد البيانات الأمنية وجمعها وتصنيفها وتحليلها باستخدام أدوات وتقنيات متخصصة، وتهدف إلى تحديد التهديدات الأمنية الحالية والناشئة، وتقييم مصادرها ودوافع الجهات الفاعلة وأساليبها وتقنياتها وإجراءاتها، لإنشاء مؤشرات تنبؤية واستخبارات أمنية قابلة للتنفيذ، بما يدعم اتخاذ القرارات الأمنية الاستباقية ويعزز قدرات الكشف المبكر والاستجابة الفعّالة، ويسهم في رفع مستوى الأمن السيبراني وحماية أصول المعلومات لمتلقي الخدمة .

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 الأمن السيبراني المُدارة، 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 الأمن السيبراني المُدارة.
٣- وصف فني لآلية تقديم خدمة الأمن السيبراني المُدارة 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 مركز العمليات مرفقة بها سيرهم الذاتية وصور مصدقة عن الشهادات والوثائق التي تثبت خبراتهم في تقديم خدمة الأمن السيبراني المُدارة.
٥- قائمة الأدوات والبرمجيات التي سيستخدمها مقدم الخدمة عند تقديم الخدمة ومميزاتها، ومكان الاستضافة، على أن تكون هذه الأدوات والبرمجيات من مصدر موثوق.
٦- شهادات اعتماد سارية المفعول صادرة عن المركز في حال سبق الحصول عليها تخول فريق مركز العمليات تقديم الخدمة.
٧- عقد العمل أو الاتفاقية الموقعة مع فريق مركز العمليات.
٨- أي شهادات اعتماد دولية سارية المفعول في مجال تقديم خدمة الأمن السيبراني المُدارة حصل عليها مقدم طلب الترخيص.
٩- وصل مقبوضات بدل دراسة طلب تقديم خدمة الأمن السيبراني المُدارة.
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 - يُشترط في تقديم خدمة الأمن السيبراني المُدارة توافر ما يلي: -
أ- اعتماد منهجية واضحة وخطط معتمدة لدى مقدم الخدمة لإدارة فريق مركز العمليات، على أن تكون متوافقة مع كلٍّ مما يلي: -
١- الإطار الوطني للأمن السيبراني.
٢- إطار الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا (NIST).
٣- أيّ معايير أخرى يعتمدها المركز.
ب- إجراءات تشغيل قياسية تُحدد العمليات الفنية والإدارية لفريق مركز العمليات، وأن تتضمن كحد أدنى ما يلي: -
١- مراقبة الأصول الرقمية وجمع البيانات ذوات الصلة.
٢- الكشف عن مؤشرات الأنشطة المشبوهة.
٣- فرز التنبيهات الواردة وتحديد أولوياتها.
٤- تحليل التنبيهات الواردة والتحقق من وجود حوادث أو هجمات سيبرانية.
٥- التعامل مع الحوادث والهجمات السيبرانية.
٦- جمع معلومات الاستخبارات السيبرانية وتحليلها.
٧- اكتشاف الثغرات الأمنية.
ج- توثيق ما يلي: -
١- نطاق خدمات مركز العمليات وتحديد مسؤولياته والتزاماته.
٢- أدوار ومسؤوليات فريق مركز العمليات وخطة التواصل.
٣- إجراءات ومؤشرات قياس أداء مركز عمليات التحليل والمراقبة.

٤- احتمالات الهجمات السيبرانية والمؤشرات المحتملة لحدوثها، وآليات اكتشافها واستراتيجيات التعامل معها.
٥- المعايير التي يتم على أساسها فرز التنبيهات الأمنية وتقييمها.
٦- معايير وآليات الإشعار بتفعيل إجراءات الاستجابة لحوادث الأمن السيبراني.
٧- معايير تصنيف الثغرات الأمنية وتحديد خطورتها.

د- خطة وإجراءات جمع البيانات على أن تتضمن تحديد البيانات المستهدفة بالرقابة، ومصادرها والآليات اللازمة لذلك حداً أدنى.

هـ- حماية مقدم الخدمة للأدوات والتجهيزات التي يستخدمها فريق مركز العمليات والإبقاء عليها سليمة وفعالة.

و- قدرة مقدم الخدمة على توفير خدمة الأمن السيبراني المُدارة على مدار الساعة، وطوال أيام الأسبوع، وعلى مدار السنة.

ز- الخطط والتدابير اللازمة لضمان استمرارية أعمال مركز العمليات ومقاومة الكوارث.

ح- حصول مقدم الخدمة على الصلاحيات اللازمة لتقديم خدمة الأمن السيبراني المُدارة من جميع الأطراف ذوات الصلة بما فيهم متلقو الخدمة وأي جهة أخرى مالكة لأحد أصول المعلومات المشمولة بنطاق الخدمة.

المادة ٥-يُشترط في الأدوات والبرمجيات والأجهزة المستخدمة لتقديم خدمة الأمن السيبراني المُدارة ما يلي: -

أ- توافر الخصائص الأمنية اللازمة بما في ذلك تخزين البيانات والاحتفاظ بها واستعادتها والمحافظة على سلامتها والتحكم في النسخ الاحتياطية من خلال جمعها وتحليلها وتوفير السجلات المناسبة والتحكم في الوصول إليها، والتحقق من الهوية والصلاحيات.

ب-القدرة على القيام بمجموعة متنوعة من المهام الحيوية بما فيها الرقابة على مختلف أصول المعلومات وإدارة المعلومات والأحداث الأمنية، وتحليل البرمجيات الخبيثة، وتحليل سلوكيات المستخدمين، والمسوحات الأمنية، وإدارة معلومات التهديدات الاستخباراتية وإجراءات مركز العمليات.

ج-القدرة على إتاحة إمكانيات المراجعة والتحليل بشكل فوري أو بشكل لاحق، وإصدار التقارير والتمثيلات البيانية والتنبيهات، والتحكم في التغييرات التي ينفذها فريق مركز العمليات، والمراقبة على أنشطتهم.

المادة ٦ -أ-يشترط في فريق مركز العمليات أن يكونوا من ذوي الخبرة والاختصاص والكفاءة، على أن لا يقل عددهم عن (١٢) اثني عشر عضوا موزعين على ثلاث مناوبات، وبحد أدنى (٤) أربعة أعضاء لكل مناوبة، ويتولى أحدهم رئاسة الفريق وإدارته في كل مناوبة وذلك في حال اعتماد نموذج المراقبة على مدار الساعة طوال أيام الأسبوع، وبخلاف ذلك يحدد المركز العدد المناسب لفريق مركز العمليات.

ب- يشترط في رئيس فريق مركز العمليات ما يلي: -

١- أن يكون حاصلاً على الشهادة الجامعية الأولى حداً أدنى في مجال تكنولوجيا المعلومات أو في أي تخصص ذي صلة.
٢- أن تكون لديه خبرة عملية في مجال الأمن السيبراني لا تقل عن (٥) خمس سنوات على أن تكون (٣) ثلاث سنوات منها في مجال خدمة الأمن السيبراني المُدارة.
٣- أن يكون حاصلاً على شهادة مهنية واحدة على الأقل من الشهادات المهنية المعتمدة لدى المركز والمنشورة على الموقع الإلكتروني الخاص به على أن يتم تحديثها باستمرار.

ج- يُشترط في أعضاء فريق مركز العمليات ما يلي:-

١- الحصول على الشهادة الجامعية الأولى أو شهادة الدبلوم المتوسط حداً أدنى من جامعة أو من جهة أكاديمية معترف بها.

٢- خبرة عملية في مجال الأمن السيبراني على أن لا تقل عن (٦) أشهر للمستوى الأول من أعضاء الفريق وفي مجال تقديم خدمة الأمن السيبراني المُدارة، ويقصد بالمستوى الأول، المستوى المسؤول عن المراقبة المستمرة للتنبيهات والأحداث الأمنية على مدار الساعة من خلال أنظمة المراقبة الأمنية، والتحقق الأولي من صحتها لتمييز الحوادث الحقيقية وغير الحقيقية، وتوثيق الحوادث الأولية، وتصعيد الحوادث التي تتطلب تحقيقاً فنياً مُعمقاً إلى المستوى الثاني وفقاً للإجراءات المعتمدة.

٣- خبرة عملية لا تقل عن (٢) سنتين للمستوى الثاني من أعضاء الفريق وفي مجال تقديم خدمة الأمن السيبراني المُدارة، ويقصد بالمستوى الثاني، المستوى المسؤول عن التحقيق والتحليل العميق للحوادث الأمنية المصعدة من المستوى الأول، وتحديد أبعادها ومصدرها، وتقديم التوصيات والإجراءات الواجب مشاركتها مع الجهات المتضررة، وتزويد فرق الاستجابة بالمعلومات اللازمة، ومراجعة وتطوير قواعد الكشف بما يحسّن كفاءة أنظمة المراقبة.

٤- الحصول على شهادة مهنية واحدة على الأقل معتمدة لدى المركز والمنشورة على الموقع الإلكتروني الخاص به على أن تكون سارية المفعول.

المادة ٧ - يلتزم مقدم خدمة الأمن السيبراني المُدارة بما يلي:

أ- الحصول على ترخيص خدمة الأمن السيبراني المُدارة ولا تخوله تقديم أي من خدمات الأمن السيبراني الأخرى التي لها تعليمات ترخيص خاصة، ويجب الحصول على ترخيص خاص بها وفق التعليمات الصادرة عن المجلس لهذه الغاية.

ب-مراعاة كفاءة فريق مركز العمليات وخبراتهم وتناسبها مع طبيعة ونطاق الخدمات المطلوبة وتصميم برنامج تدريبي وتنفيذه لتطوير مهارات الفريق بشكل مستمر.

ج-الفصل ما بين بيانات متلقي الخدمة على مستوى قواعد البيانات، للحفاظ على الخصوصية والسرية.

د-حماية أنظمة متلقي الخدمة التي تتم إدارتها في مركز العمليات وعزلها.

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

و- تقديم الخدمة بأمانة ونزاهة واحترافية، والامتناع عن تقديم معلومات غير صحيحة أو مضللة وعدم استخدام الرُخصة لأغراض أخرى غير تلك الممنوحة من أجلها، تحت طائلة المساءلة القانونية.

ز-تزويد المركز بتقارير سنوية إحصائية تتضمن معلومات عن المستفيدين من الخدمة، والخدمات المقدمة لهم وأي قضايا أو حوادث رئيسة ذوات صلة، وحفظ هذه التقارير بشكل آمن وحماية الوصول إليها.

ح-عدم التعاقد من الباطن لتقديم خدمة الأمن السيبراني المُدارة إلا مع جهة مرخصة وفق الأصول من المركز.

ط-الربط والتكامل مع أنظمة المركز ومنصاته بهدف إدارة وأتمتة الإجراءات وتزويد المركز بالمعلومات التي يحتاجها للقيام بمسؤولياته أو بأي طريقة يراها المركز مناسبة.

ي-التعاون مع المركز خلال عمليات التدقيق التي يقوم بها وتزويده بأي معلومات أو وثائق يراها ضرورية.

المادة ٨ - مع مراعاة أحكام هذه التعليمات، على مقدم خدمة الأمن السيبراني المُدارة عند تقديمه الخدمة الالتزام بما يلي:

أ-تحديد آليات التنسيق مع متلقي الخدمة وتحديد جهات التواصل بما في ذلك الإبلاغ عند حدوث أي طارئ أو حادث أمن سيبراني.

ب-تحديد أصول المعلومات المشمولة بخدمات مركز العمليات، والاحتفاظ بسجل للأصول وتحديثه باستمرار.
ج-توفير واستخدام الآليات والأساليب المناسبة لمراقبة أصول المعلومات وتحليل المعلومات والاستجابة المناسبة للأحداث والتنبيهات الآلية الواردة.
د-استخدام الأساليب المناسبة لتحليل البيانات والأحداث الأمنية ومعلومات الاستخبارات السيبرانية .
هـ-تحديد تواتر عمليات المراقبة والتحليل والفحص.
و-تحديد جدول المناوبات لفريق مركز العمليات وتحديد أعضائه لكل مناوبة.
ز-تحديد التقارير والمعلومات المتضمنة فيها، والجهات المستهدفة ومعدل إصدارها.
ح-ضبط التجهيزات والأدوات والأنظمة بما يحسن جودة بيانات وعمليات المراقبة والتحليل والفحص وأداء مركز العمليات بشكل مستمر.
ط-تحديد آليات التنسيق مع الفرق والأطراف الأخرى حسب مقتضى الحال مثل فريق التحقيق الجنائي الرقمي وفريق الاستجابة لحوادث الأمن السيبراني.
ي-اتخاذ الإجراءات اللازمة لاكتشاف الثغرات الأمنية، والإبلاغ عنها.
ك- الالتزام بالمعايير المعتمدة والمنصوص عليها في كافة التشريعات النافذة والمتعلقة بالأمن السيبراني، وبالإطار الوطني للأمن السيبراني.
ل-الالتزام بالمعايير المهنية والأخلاقية، وأداء الواجبات بموضوعية، وبذل العناية الواجبة.
م-اتخاذ الإجراءات اللازمة لحماية أصول وأنظمة متلقي الخدمة، وعدم إلحاق الضرر بها أو إساءة استخدام المعلومات التي يحصل عليها.
ن- جمع ومعالجة بيانات متلقي الخدمة المتعلقة بتقديم الخدمة فقط.
س-إعلام متلقي الخدمة بأي مشاهدات أو ثغرات أمنية يتم رصدها خلال تقديم الخدمة، والتي قد تؤثر في سلامة متلقي الخدمة وأمنه وسمعته.
ع-تزويد متلقي الخدمة بالمخرجات والتقارير وقياسات الأداء وفق ما هو محدد في الاتفاقية المبرمة.
ف-عدم تضمين المعلومات الحساسة والسرية في التقارير، أو إخفائها لمنع استغلالها.

المادة ٩- يلتزم مقدم خدمة الأمن السيبراني المُدارة بإبلاغ المركز عن أي من الحالات التالية: -
أ- فقدان أي شرط من شروط أو متطلبات الترخيص المنصوص عليها في النظام.
ب- أي تغيير يطرأ على فريق مركز العمليات، 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 الأمن السيبراني المُدارة إلى آخر.
ج-أي تغيير يؤثر على قدرة وكفاءة مقدم الخدمة على تقديمها.
د- الحصول على معلومات أثناء تقديم الخدمة تشير إلى قيام متلقي الخدمة بارتكاب مخالفة لأحكام القانون أو الأنظمة أو التعليمات الصادرة بمقتضاه.

المادة ١٠-أ- على مقدم خدمة الأمن السيبراني المُدارة الاحتفاظ بالمعلومات المتعلقة بخدمة الأمن السيبراني المدارة لمدة لا تقل عن (٣) ثلاث سنوات من تاريخ الانتهاء من تقديمها على أن تتضمن ما يلي:-
١- أسماء ومعلومات فريق مركز العمليات الذين شاركوا في تقديم الخدمة.
٢- أسماء ومعلومات متلقي الخدمة وتاريخ تقديم الخدمة ومدتها.
٣- التقنيات والأدوات المستخدمة.
٤- أي معلومات أخرى يطلبها المركز.
ب- على الرغم مما ورد في الفقرة (أ) من هذه المادة على مقدم الخدمة الاحتفاظ بالمعلومات المتعلقة بخدمة مركز العمليات بما يتوافق مع السياسات والتشريعات ذوات العلاقة و حمايتها.

المادة ١١- أ- على متلقي خدمة الأمن السيبراني المُدارة الالتزام بما يلي: -
١-عدم التعاقد على تقديم الخدمة إلا مع مقدم خدمة مرخص وفقاً لأحكام النظام والتعليمات الصادرة بمقتضاه.
٢-التأكد من حصول فريق مركز العمليات على شهادات مصدقة من المركز قبل تقديم الخدمة.
٣-تزويد مقدم الخدمة بالمعلومات والمتطلبات التي يحتاجها لتقديم الخدمة.
٤-إبلاغ المركز عن أي إخلال من مقدم الخدمة بأي من المتطلبات المنصوص عليها في هذه التعليمات.
ب- لمتلقي الخدمة استشارة المركز فنياً قبل توقيع اتفاقية خدمة مع أيٍ من مقدمي خدمة الأمن السيبراني المُدارة المُرخصين.
المادة ١٢- لغايات تنفيذ أحكام هذه التعليمات، يتولى المركز القيام بما يلي: -
أ-إجراء التدقيق السنوي على مقدمي الخدمة المُرخصين للتحقق من الامتثال 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 التراخيص وحالتها (فعّال، أو موقوف، أو ملغى) وخبراتهم ومعلومات التواصل الخاصة بهم .
ج-توثيق أي إجراءات تأديبية أو عقوبات يتم اتخاذها بمقدم الخدمة المرخص في السجل العام.
المادة ١٣- 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 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 الأمن السيبراني المدارة المعمول بها بناء على شكوى من متلقي الخدمة.
ز-إذا صدر بحقه حكم قضائي قطعي يقضي بإيقاف ترخيص مقدم الخدمة أو تعديله أو إلغاؤه .
ح-إذا اقتضت المصلحة العامة ذلك.
المادة ١٤- أ- تكون مدة الترخيص لخدمة الأمن السيبراني المُدارة (٣) 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 ١٥ - 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

نظام ترخيص مقدمي خدمات الأمن السيبراني رقم76 لسنة 2024

المنشور على الصفحة 6429 من عدد الجريدة الرسمية رقم 5962 بتاريخ2024/11/17

صادر بموجب الفقرة 2 من المادة 6 من قانون الامن السيبراني رقم 16 لسنة 2019

صادر بموجب المادة 18 من قانون الامن السيبراني رقم 16 لسنة 2019

المادة 15

يصدر المجلس التعليمات اللازمة لتنفيذ أحكام هذا النظام بما في ذلك التعليمات الناظمة لكل خدمة من خدمات الأمن السيبراني والإجراءات والمتطلبات اللازمة للعمل بها على أن تتضمن معايير تقديم خدمات الأمن السيبراني والشروط والمؤهلات الواجب توافرها في مقدمي الخدمة.

22/10/2024