تعليمات ترخيص خدمة تدقيق 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 تدقيق الأمن السيبراني 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 تدقيق الأمن السيبراني : عملية تتضمن مراجعة وفحص أصول المعلومات الرقمية وغير الرقمية بشكل منظم وموثق وموضوعي ومستقل بهدف تقييم مدى حمايتها واكتشاف الثغرات الأمنية وتقييم مدى الامتثال للمعايير والسياسات المعتمدة في مجال الأمن السيبراني.

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 أو تأثيرات وعواقب أمنية غير مرغوبة على أصول المعلومات.

الإخلالات الأمنية : أي حادث يتمكن فيه طرف غير مصرح له من اختراق آليات الحماية والنفاذ إلى أصول المعلومات بقصد التسبب بأضرار أو انتهاكات أمنية ويشمل ذلك سرقة البيانات أو تسريبها.

نقاط الضعف : مواطن الضعف في أصول المعلومات ، التي يمكن استغلالها من خلال التهديدات والإخلالات الأمنية.

مدقق الأمن السيبراني : خبير أو مجموعة من الخبراء لدى مقدم الخدمة معنيون بتقديم خدمة تدقيق الأمن السيبراني لمتلقي الخدمة، ولديهم المؤهلات، والخبرات والمهارات والكفاءات اللازمة لأداء مهامهم، ويتميزون بالموضوعية والنزاهة والاستقلالية المطلوبة.

المخاطر : أي حدث أو فعل أو ضرر محتمل يلحق بالأشخاص أو الممتلكات أو البيانات أو الأنظمة، نتيجة خلل أو تهديد داخلي أو خارجي أو عدم الالتزام بالتشريعات ذوات العلاقة.

غرفة تجارة عمان AMMAN CHAMBER OF COMMERCE
التاريخ: ٢٠٢٦/٠٣/٢٥
رقم الوارد: ١١٨٠

مخـــاطر الأمـــن السيبراني : الأحداث المحتملة التي قد تتسبب في ضرر أو تؤثر سلباً على الأصول من حيث سرّيتها أو سلامتها أو توفرها، نتيجة استغلال ثغراتها الأمنية من خلال التهديدات والإخلالات الأمنية.

مخاطر التدقيق : توصل المدقق إلى نتيجة غير صحيحة أو عدم اكتشافه للثغرات الأمنية والإخلالات الأمنية.

الأدلة : البيانات والمعلومات التي يقوم بجمعها المدقق ويوثقها أثناء التدقيق لدعم الاستنتاجات والنتائج التي يتوصل إليها.

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

المادة٣ - على مقدم طلب الحصول على ترخيص خدمة تدقيق 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 تدقيق الأمن السيبراني.

٣- وصف فني لآلية تقديم خدمة تدقيق 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 مدققي الأمن السيبراني مرفقة بها سيرهم الذاتية وصور عن الشهادات المصدقة والوثائق التي تثبت خبراتهم في تقديم خدمة تدقيق الأمن السيبراني.

٥- شهادات اعتماد سارية المفعول صادرة عن المركز في حال سبق الحصول عليها تخول مدقق الأمن السيبراني تقديم الخدمة.

٦- عقد العمل أو الاتفاقية الموقعة مع مدقق الامن السيبراني لتقديم خدمة تدقيق الأمن السيبراني.

٧- أي شهادات اعتماد دولية سارية المفعول في مجال تقديم خدمة تدقيق الأمن السيبراني حصل عليها مقدم طلب الترخيص.

٨- وصل مقبوضات بدل دراسة طلب تقديم خدمة تدقيق الأمن السيبراني.

٩- قائمة أدوات وبرمجيات التدقيق التي سيستخدمها مقدم الخدمة عند تقديم الخدمة ومميزاتها، ومكان الاستضافة، على أن تكون تلك الأدوات والبرمجيات من مصدر موثوق.

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 وذلك للتحقق من صحة المعلومات المقدمة وتقييم إمكاناته وقدراته.

المادة ٤ -أ-يُشترط في تقديم خدمة تدقيق الأمن السيبراني أن تتوافق مع ما يلي:-
١-الإطار الوطني للأمن السيبراني.
٢-معايير وإرشادات التدقيق المعتمدة دوليا بما فيها معايير وإرشادات تدقيق تقنية المعلومات (ITAF)الصادرة عن جمعية تدقيق ومراقبة نظم المعلومات (ISACA)، والمعايير (ISO٢٧٠٠٧/ISO١٩٠١١) الصادرة عن المنظمة الدولية للمعايير والدليل الإرشادي (SP ٨٠٠-٥٣) الصادر عن المعهد الوطني للمعايير والتكنولوجيا (NIST).
٣-أي معايير أخرى يعتمدها المركز.
ب- يشترط أن تتضمن منهجية تدقيق الأمن السيبراني ما يلي: -
١- إعداد خطة التدقيق وتقييم المخاطر ذوات الصلة.
٢- تحديد الضوابط وفق نطاق التدقيق وهدفه ونتائج تقييم المخاطر.
٣- تحديد المعايير التي سيتم تطبيقها عند تنفيذ التدقيق وعمليات التقييم.
٤- تقييم الضوابط المطبقة من حيث الكفاءة والفعالية وجمع الأدلة الداعمة.
٥- توثيق الأعمال المنجزة ونتائج التدقيق.
٦- التأكد من صحة نتائج التدقيق بالتنسيق مع المعنيين لدى متلقي الخدمة.
٧- إعداد تقرير التدقيق ومناقشته.
ج- يشترط تحديد وتقييم وتوثيق جميع المخاطر المتعلقة بتدقيق الأمن السيبراني بما فيها مخاطر الأمن السيبراني ومخاطر التدقيق باستخدام منهجيات مناسبة لتقييم المخاطر وتخفيضها والتركيز على الجوانب الأكثر خطورة.
د- أن تكون معايير التقييم المستخدمة ملائمة لهدف ونطاق التدقيق وموثوقة ومفهومة، ومقبولة لدى متلقي الخدمة بما يضمن تقييماً متسقاً وعادلاً وموضوعياً.
هـ- توفير الإشراف الكافي لضمان تنفيذ خدمة التدقيق بطريقة مهنية ووفقاً للأحكام المنصوص عليها في هذه التعليمات مع الامتناع عن تقديم الخدمة في حال عدم استيفاء المتطلبات اللازمة لذلك.
و- على مقدم الخدمة توثيق نتائج التدقيق وإبلاغ المركز بها في أسرع وقت ممكن إذا اقتضت طبيعة التدقيق ذلك وبناءً على أهميتها.
ز- تحدد مدة إجراء التدقيق وفقا لمتطلبات الإطار الوطني للأمن السيبراني.
المادة ٥- يشترط في مدقق الأمن السيبراني أن يكون:-
أ- حاصلاً على الشهادة الجامعية الأولى حدا أدنى في تكنولوجيا المعلومات أو أي تخصص ذي علاقة.
ب-حاصلاً على شهادة مهنية واحدة على الأقل معتمدة لدى المركز والمنشورة على موقعه الالكتروني.
ج- لديه خبرة عملية في مجال الأمن السيبراني لا تقل عن (٥) خمس سنوات، منها (٣) ثلاث سنوات على الأقل في مجال خدمة تدقيق الأمن السيبراني.

المادة ٦ -يلتزم مقدم خدمة تدقيق الأمن السيبراني بما يلي: -

أ-التأكد من توافر الكفاءة والخبرة المناسبة لدى مدقق الأمن السيبراني بما يتناسب مع هدف التدقيق ونطاقه المطلوب، وتصميم وتنفيذ برنامج تدريبي مستمر لتطوير مهارات الفريق.

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

ج- تقديم الخدمة بأمانة ونزاهة واحترافية، والامتناع عن تقديم معلومات غير صحيحة أو مضللة، وعدم استخدام الرُخصة لغير الأغراض الممنوحة لأجلها ، تحت طائلة المساءلة القانونية.

د- تزويد المركز بتقارير إحصائية سنوية تتضمن معلومات عن المستفيدين من الخدمة، والخدمات المقدمة لهم ، وأي قضايا أو حوادث رئيسة ذوات صلة، وحفظ هذه التقارير بصورة آمنة وضمان حماية الوصول إليها.

هـ- الامتناع عن التعاقد من الباطن لتقديم خدمة تدقيق الأمن السيبراني إلا مع جهة مرخصة وفق الأصول من المركز.

و-الربط والتكامل مع أنظمة المركز ومنصاته بهدف إدارة وأتمتة الإجراءات وتزويد المركز بالمعلومات التي يحتاج اليها للقيام بمسؤولياته بالطريقة التي يراها المركز مناسبة.

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

المادة ٧- مع مراعاة أحكام هذه التعليمات، يلتزم مقدم خدمة تدقيق الأمن السيبراني عند تقديم الخدمة بما يلي:-

أ- عدم تقديم الخدمة لأي جهة تكون له معها أي مصلحة مالية، مباشرةً أو غير مباشرة أو عمل معها في مشاريع تنفيذية سابقة لتقديم الخدمة.

ب-إعداد خطة تدقيق الأمن السيبراني، على أن تتضمن على الأقل ما يلي: -

١- هدف التدقيق ونطاقه.

٢- فريق العمل والأدوار والمسؤوليات.

٣-الجدول الزمني.

٤-برنامج التدقيق.

٥-الأدوات والتقنيات اللازمة.

ج-التأكد من تنفيذ جميع إجراءات التدقيق اللازمة وفقاً لخطة التدقيق، بحيث تشمل المخاطر المحددة وتلتزم بالجدول الزمني المتفق عليه.

د-الحصول على الأدلة المناسبة والموثوقة والكافية لدعم الاستنتاجات ونتائج التدقيق.

هـ-توثيق عملية التدقيق بما في ذلك هدف التدقيق ونطاقه، وخطة وبرنامج التدقيق، والأدوات المستخدمة، والنتائج، والتوصيات، والأدلة الداعمة، والاحتفاظ بها وفقاً للأحكام هذه التعليمات.

و-اتخاذ جميع الإجراءات اللازمة لضمان حماية أصول وأنظمة متلقي الخدمة، وعدم إلحاق الضرر بها أو إساءة استخدام المعلومات التي يحصل عليها.

ز- جمع بيانات متلقي الخدمة ومعالجتها لأغراض محددة وصريحة تتعلق بتقديم الخدمة فقط.
ح-إعلام متلقي الخدمة بأي مشاهدات أو ثغرات أمنية يجدها خلال تقديم الخدمة قد تؤثر على سلامة متلقي الخدمة وأمنه وسمعته.
ط-تزويد متلقي الخدمة بتقرير عن خدمة تدقيق الأمن السيبراني على أن يتضمن، كحد أدنى، المعلومات التالية :-
١- هدف التدقيق ونطاقه.
٢- الفترة المشمولة وتاريخ إصدار التقرير.
٣- أي قيود على تداول التقرير و مشاركته.
٤- ملاحظات التدقيق ودرجة خطورتها وتأثيرها.
٥-توصيات التدقيق.
٦-توقيع المدقق.
ي-مناقشة نتائج التدقيق وملاحظات مدقق الخدمة ، مع المعنيين لدى متلقي الخدمة ، وتضمين ردودهم في تقرير التدقيق النهائي.

المادة ٨- يلتزم مقدم خدمة تدقيق الأمن السيبراني بإبلاغ المركز عن أي من الحالات التالية:-
أ- فقدان أي شرط من شروط الترخيص ومتطلباته المنصوص عليها في النظام أو هذه التعليمات .
ب- أي تغيير يطرأ على مدقق الأمن السيبراني، ويحظر على أي مدقق أمن سيبراني جديد تقديم الخدمة إلا بعد الحصول على شهادة من المركز تخوله ذلك، وتبقى الشهادة مرتبطة به ولا تتأثر حال انتقاله من أحد مقدمي خدمة تدقيق الأمن السيبراني إلى آخر.
ج-أي تغيير يؤثر في 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.

المادة٩ - أ- على مقدم الخدمة الاحتفاظ بالمعلومات المتعلقة بخدمة تدقيق الأمن السيبراني لمدة لا تقل عن (٣) ثلاث سنوات من تاريخ الانتهاء من تقديمها، على أن تتضمن ما يلي: -
١- أسماء ومعلومات مدققي الأمن السيبراني الذين شاركوا في تقديم الخدمة .
٢- أسماء ومعلومات متلقي الخدمة وتاريخ تقديم الخدمة ومدتها.
٣- معلومات خدمة التدقيق المقدمة وتشمل ما يلي:-
أ-هدف التدقيق ونطاقه.
ب-خطة التدقيق.
ج-الاختبارات المنفذة والعينات المأخوذة حسب مقتضى الحال.
د-أي معلومات أخرى يطلبها المركز.
ب- على الرغم مما ورد في الفقرة (أ) من هذه المادة على مقدم الخدمة الاحتفاظ بالمعلومات المتعلقة بخدمة تدقيق الأمن السيبراني بما يتوافق مع السياسات والتشريعات ذوات العلاقة و حمايتها.

المادة ١٠ - أ- على متلقي خدمة تدقيق الأمن السيبراني الالتزام بما يلي: -
١-عدم التعاقد على تقديم الخدمة إلا مع مقدم خدمة مرخص وفقاً لأحكام النظام والتعليمات الصادرة بمقتضاه.
٢-التأكد من حصول مدققي خدمة الأمن السيبراني على شهادات مصدقة من المركز قبل تقديم الخدمة.
٣-تزويد مقدم الخدمة بالمعلومات والمتطلبات التي يحتاج اليها لتقديم الخدمة.
٤-إبلاغ المركز بأي 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 تدقيق الأمن السيبراني المُرخصين.
المادة ١١ - 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 تقديم 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 بمقدم الخدمة المرخص في السجل العام.

المادة ١٢ - 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 تدقيق 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.

المادة١٣-أ-تكون مدة الترخيص لخدمة تدقيق الأمن السيبراني (٣) ثلاث سنوات تبدأ من تاريخ إصدار الترخيص وتجدد لمدة مماثلة وفقاً لأحكام النظام.

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

المادة١٤-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

مركز عدالة للمعلومات القانونية
ADALEH Center for Legal Information
Info@Adaleh.Info

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