الضوابط والنواظم الخاصة
باعتمادية شركات خدمات أمن المعلومات

التصنيف: عام

الإصدار: ١

٢٠٢٠

ضبط الوثيقة

سجل التغيرات

التاريخ	المعدل	النسخة	ملاحظات
٢٠١٩/١١/١	م.مادلين الشلي	٠,١	Vol_١_credit_ISC_v_٠,١-١-١١-٢٠١٩
٢٠١٩/١١/١٩	مديرية التنظيم والتراخيص مركز أمن المعلومات	٠,٢	
٢٠١٩/١١/٢٦	مديرية التنظيم والتراخيص	٠,٣	
٢٠١٩/١٢/١٦	المدير العام–م. علي علي مديرية التنظيم والتراخيص مركز أمن المعلومات	٠,٤	
٢٠٢٠/١/١٣	مديرية التنظيم والتراخيص مركز أمن المعلومات	٠,٥	
٢٠٢٠/١/١٤	مديرية التنظيم والتراخيص مركز أمن المعلومات	٠,٦	
٢٠٢٠/١/١٥	المدير العام–م. علي علي مديرية التنظيم والتراخيص مركز أمن المعلومات	٠,٧	
٢٠٢٠/١/١٦	المدير العام–م. علي علي	١,٠	

مراجعة الوثيقة

تم إرسال هذه الوثيقة إلى الأشخاص التاليين للمراجعة وتقديم آرائهم عليها:

التاريخ	الاسم	الصفة	الملاحظات
١٩/١/٢٠٢٠	م. علي علي	المدير العام	
٢٨/١/٢٠٢٠		مجلس الإدارة	

جدول المحتويات

المادة ١: تعاريف

إضافة إلى التعاريف الواردة في قانون التوقيع الإلكتروني وخدمات الشبكة رقم/٤/ للعام ٢٠٠٩، يكون للمصطلحات والتعابير الآتية المعاني المبينة بجانب كل منها عند تطبيق بنود هذه الوثيقة:

الهيئة: الهيئة الوطنيّة لخدمات الشّبكة.

أمن المعلومات: الوسائل والتّدابير الخاصة بالحفاظ على سريّة، وتوافُريّة، وسلامة المعلومات، وحمايتها من الأنشطة غير المشروعة التي تستهدفها.

الوثيقة: اللائحة التنظيمية المتضمنة اعتمادية شركات خدمات أمن المعلومات، وهي هذه الوثيقة.

الاعتمادية: موافقة الجهة الإدارية المختصة والمشرفة على نشاط ما بمنح الإذن لجهة خاصة بممارسة هذا النشاط إذا تحققت فيها الشروط اللازمة لذلك.

تطوير سياسة أمن المعلومات: إعداد السياسة الأمنية الخاصة بجهة ما وفق معايير أمن المعلومات التي تحددها هذه الجهة.

تدقيق أمن نظم المعلومات: تدقيق مدى تطبيق الإجراءات المتعلقة بأمن المنظومة المعلوماتية استناداً إلى الوثائق التي تعرف تلك الإجراءات، وذلك بهدف التأكد أن ما أقرته المؤسسة من تعليمات وسياسات وخطط لأمن المعلومات مطبق فعلياً ويتم الالتزام به، وتحديد حالات عدم الالتزام.

وضع خطط التعامل مع الحوادث الطارئة: وضع مجموعة العمليات المنهجة لإدارة ومعالجة تداعيات خرق أمني أو هجوم إلكتروني أو أي حادث طارئ تتعرض له منظومة معلوماتية ما.

تقييم المخاطر: الإجرائية المتكاملة التي تسمح بتحديد الأخطار التي يمكن أن تتعرض لها المنظومة والآثار التي يمكن أن تنتج عنها واقتراح الإجراءات اللازمة بهدف مساعدة الإدارة على اتخاذ القرارات المناسبة للتعامل مع تلك الأخطار.

تقييم الثغرات الأمنية: عملية البحث والتقصي عن جميع الثغرات ونقاط الضعف المحتملة في منظومة معلوماتية وذلك بغرض تصنيفها وتحليلها وتقييمها.

اختبار الاختراق: خدمة متقدمة تتضمن خدمة المسح الأمني الاحترافي ويُضاف إليها اختبار اختراق منظومات الزبون بطرق تحاكي هجوم حقيقي بالتنسيق مع الزبون ولا تسبب ضرراً لأنظمته.

استعادة بيانات مفقودة: استعادة بيانات تعذر الوصول إليها أو تم فقدانها نتيجة خلل ما، وإعادتها لوضعها الطبيعي لما قبل حدوث العامل المسبب على وسائط التخزين المختلفة.

مراجعة الكود أمنياً: مراجعة الرِماز المصدري من منظور أمني بهدف اقتراح التعديلات البرمجية التي تضمن عمل التطبيق بشكل آمن.

الخصوصيّة: حق الفرد في حماية أسراره الشخصيّة والملاصقة للشخصيّة والعائليّة ومراسلاته وسمعته وحرمة منزله وملكيته الخاصّة وفي عدم اختراقها أو كشفها دون موافقته.

سريّة المعلومات: ضمان عدم الكشف عن المعلومات لأشخاص أو عمليّات أو أجهزة غير مصرّح لها بذلك.

توافُريّة المعلومات: ضمان النّفاذ إلى المعلومات واستخدامها في الوقت المناسب وبشكل موثوق من قبل المخولين بذلك.

المسح الأمني: عملية البحث عن الثغرات الأمنية في المنظومات المعلوماتية.

الثغرة الأمنية: خلل أو ضعف يمكن أن تتعرض له إجراءات أو تصميم أو تنفيذ أو الضوابط الداخلية لحماية المنظومات المعلوماتية وينتج عنها خرقاً أو انتهاكاً لسياسة حماية المنظومات المعلوماتية.

الزبون: أي شخص طبيعي أو اعتباري يقوم بطلب خدمة من خدمات أمن المعلومات.

الأصول المعلوماتية: البيانات والمعلومات والبنية التحتية والبيئة المحيطة بها (من تجهيزات أو برمجيات أو خدمات أو مستخدمين أو مرافق إلخ....).

الشركة المعتمدة: شخص اعتباري حاصل على الاعتمادية من الهيئة.

المادة ٢: أحكام عامة

أ. تعتبر شروط هذه الوثيقة وكافة اللوائح التنظيمية ذات الصلة الصادرة عن الهيئة مُلزمة للشركة المعتمدة.

ب. تعتبر الاعتمادية شخصية لا يجوز التنازل عنها لأية جهة أخرى.

ج. مدة الاعتمادية **سنة ميلادية** تبدأ من تاريخ منحها.

د. كافة البيانات المتداولة بين الشركة المعتمدة والهيئة هي بيانات سرية، يتم الاحتفاظ بها بشكل آمن في الهيئة.

هـ. للهيئة تعديل هذه الوثيقة على أن تبلّغ الشركات المعتمدة بذلك، وتصبح التعديلات نافذة بانقضاء مدة ثلاثين يوماً من تاريخ نشرها.

و. تتحمل الشركة المعتمدة كامل المسؤولية القانونية أو المالية الناجمة عن الضرر المادي أو المعنوي الذي يمكن أن تتسبب به للغير في إطار الاعتمادية الممنوحة لها.

المادة ٣: نطاق الاعتمادية

يحدد نطاق الاعتمادية بتقديم خدمات أمن المعلومات في الجمهورية العربية السورية، على سبيل الذكر لا الحصر:

١. تطوير سياسة أمن المعلومات.
٢. تدقيق أمن نظم المعلومات.
٣. وضع خطط التعامل مع الحوادث الطارئة.
٤. تقييم المخاطر.
٥. تقييم الثغرات الأمنية.
٦. اختبار الاختراق.
٧. استعادة بيانات مفقودة.
٨. مراجعة الكود أمنياً.

المادة ٤: شروط الحصول على الاعتمادية

أ. شركة وطنية عاملة في مجال تقانة المعلومات والاتصالات.

ب. خبرة للشركة لا تقل عن ثلاث سنوات في حدود المادة /٣/ من هذه الوثيقة، ويمكن أن يُستعاض عن ذلك بوجود دعم موثق من شركة متخصصة (داخلية أو خارجية)، كما يؤخذ بعين الاعتبار وجود خبرات كافية ضمن الكادر التقني للشركة في ضوء الاختبارات التي ستجريها الهيئة.

ج. استخدام برمجيات لها إمكانية إصدار التقارير بشكل آلي متضمنة النتائج التي تم الحصول عليها، في الخدمات التي تتطلب ذلك.

د. لا تُقبل البرمجيات مفتوحة المصدر إلا بعد موافقة الهيئة.

المادة ٥: إجراءات الحصول على الاعتمادية

أ. تتقدم الشركة بطلب للحصول على الاعتمادية وفق الملحق /١/ ويُسجل في ديوان الهيئة.

ب. يُرفق بالطلب جميع الوثائق المطلوبة وفق الملحق /٢/.

ج. تقوم الهيئة بدراسة الطلب ومرفقاته للتأكد من توفر الشروط اللازمة.

د. تقوم الهيئة بإجراء الاختبارات اللازمة وفق الملحق /٣/ للخدمات المطلوبة.

هـ. تقوم الهيئة بإبلاغ الشركة بنتيجة الدراسة والاختبارات خلال خمسة أيام عمل من صدورها.

و. تُرسل الهيئة المطالبة للشركة لتسديد الأجور المستحقة عند الموافقة على منح الاعتمادية.

ز. تُصدر الهيئة شهادة الاعتمادية متضمنة خدمات أمن المعلومات التي تقدمها الشركة.

ح. تقوم الشركة المعتمدة باستصدار شهادة توقيع رقمي خاصة بالشركة.

ط. تحتفظ الهيئة بكافة نتائج اختبارات قبول الشركة في سجل موقع إلكترونياً من قبل الهيئة.

ي. تقوم الهيئة بنشر قرار منح الاعتمادية على الموقع الإلكتروني للهيئة.

المادة ٦: التزامات الشركة المعتمدة

أ. **تلتزم الشركة المعتمدة بالآتي:**

١. أحكام القوانين ذات الصلة والتعليمات التنفيذية واللوائح التنظيمية والقرارات الصادرة عن الهيئة.

٢. السياسة الوطنية لأمن المعلومات واللوائح التنظيمية المرتبطة بها، في حال كان الزبون هو أحد جهات القطاع العام.

٣. شروط الاعتمادية الواردة في الوثيقة.

٤. ضمان صحة جميع البيانات والمستندات الفنية والمالية والقانونية المقدمة للهيئة.

٥. تسليم الزبون التقارير النهائية للخدمات المقدمة، بما في ذلك التقارير التي تولدها أدوات الاختبار المستخدمة، وللهيئة التأكد من سلامة التقارير في حال ورود شكوى من الزبون.

٦. إدراج أسماء البرمجيات المستخدمة ضمن التقارير النهائية المسلمة للزبون، إذا كانت الخدمة تتطلب استخدام برمجيات.

٧. التحديث الدوري للبرمجيات المستخدمة من قبلها في تقديم الخدمات.

٨. إرسال تقرير دوري كل ستة أشهر يتضمن خدمات أمن المعلومات المقدمة من قبل الشركة المعتمدة وفق الملحق/٤/.

٩. الحفاظ على الخصوصية والسرية للمعلومات التي تحصل عليها الشركة المعتمدة في سياق عملها لدى الزبون.

١٠. اتخاذ جميع الإجراءات اللازمة لضمان حماية المحتوى المخزن لديها والخاص بالزبون.

١١. تقديم البيانات والمعلومات والإيضاحات التي تطلبها الهيئة المتعلقة بهذه الاعتمادية وذلك بالشكل الصحيح وفي الموعد الذي تحدده الهيئة.

١٢. تعيين العدد الكافي من العاملين بشرط ألا يكون أياً من العاملين في الشركة المعتمدة مسؤولاً عن تقديم أكثر من ٣ خدمات، مع الالتزام بوجود بديل عن كل عامل لتقديم الخدمة نفسها.

١٣. تطبيق أفضل الممارسات العالمية لتقديم خدمات أمن المعلومات.

١٤. تسليم الزبون نسخة الكترونية من النتائج التي توصل لها مقدم الخدمة.

١٥. الحصول على موافقة الهيئة على أي تعديل بقائمة العاملين المعنيين بتقديم الخدمات، الذين تم منح الاعتمادية بناءً على اختبارات أُجريت لهم حسب الخدمة المكلفين بتقديمها.

١٦. الحصول على موافقة الهيئة على أي تعديل بالأدوات والبرمجيات التي تم منح الاعتمادية وفقها.

ب. تلتزم الشركة المعتمدة بتقديم خدمات أمن المعلومات وفق ما يلي:

١. تطوير سياسة أمن المعلومات:

يجب أن تذكر الشركة المعتمدة المعيار العالمي المعتمد في تطوير السياسة والذي تم الاتفاق عليه مع الزبون بناء على احتياجاته.

٢. تدقيق أمن نظم المعلومات:

يجب أن تعتمد الشركة المعتمدة تقييم منهجي لأمن نظم معلومات المؤسسات من خلال قياس مدى توافقه مع مجموعة من المعايير القياسية، تقوم المراجعة الشاملة عادةً بتقييم أمان التكوين المادي للتجهيزات والبنية التحتية وبيئة النظام، والبرمجيات والتطبيقات، وعمليات معالجة المعلومات، وسياسات المستخدمين وتدقيق كل ذلك من وجهة نظر أمنية بحتة.

٣. **وضع خطط التعامل مع الحوادث الطارئة:**

يجب أن تتضمن هذه الخدمة بالحد الأدنى المراحل التالية وذلك وفقاً لمعايير أمن المعلومات التي تقترحها الشركة المعتمدة ويوافق عليها الزبون:

أ. **مرحلة التحضير:** تدريب العاملين بشكل صحيح ومسبق فيما يتعلق بأدوارهم ومسؤولياتهم تجاه الاستجابة للحالات الطارئة وإعداد وتطوير سيناريوهات لحالات طارئة تحاكي حالات طارئة حقيقية والتدريب عليها بما يناسب التعامل مع كل حالة طارئة والتأكد من توثيق خطة الاستجابة ورصد الاعتمادات المالية الكافية لتمويلها. كذلك التأكد من وجود وسلامة النسخ الاحتياطية للبيانات وإعدادات المنظومة المعلوماتية واختبارها وجاهزية مواقع التشغيل البديلة إن وجدت.

ب. **مرحلة الكشف والتحليل:** القيام بالكشف على الحادث الطارئ والتأكد من حدوثه وتحديد نوعه ونطاق تأثيره ضمن المنظومة المعلوماتية والأسباب التي أدت إلى حدوثه.

ج. **مرحلة الاحتواء:** مجموعة الإجراءات التي تهدف لمنع انتشار الضرر الذي سببه وقوع الحادث الطارئ وتخفيف آثاره إلى أقصى حد، وتتضمن أيضاً تشغيل المنظومات المعلوماتية الاحتياطية (في حال توفرها) لاستعادة العمل ريثما يتم إعادة المنظومات المعلوماتية الرئيسية إلى العمل.

د. **مرحلة جمع الأدلة الرقمية:** في حال كان الحادث الطارئ ناجم عن جريمة معلوماتية يتم جمع الأدلة الرقمية وتوثيقها.

هـ. **مرحلة معالجة الحادث الطارئ:** معالجة الأسباب والتهديدات الأمنية التي أدت إلى وقوع الحادث الطارئ بما يتناسب مع نوعه وتصنيفه وضمان سلامة المنظومة المعلوماتية لتعود للعمل بشكل طبيعي.

و. **مرحلة الاستعادة:** إعادة المنظومة للعمل إلى حالتها الطبيعية قبل وقوع الحادث الطارئ وما يرافق ذلك من عمليات استعادة للبيانات سواء من النسخ الاحتياطية أو بأدوات استعادة البيانات المفقودة.

ز. **مرحلة استخلاص الدروس:** بعد استعادة العمل بشكل طبيعي يتم عقد اجتماع بين إدارة الجهة وفريق الاستجابة لديها لمناقشة الدروس والنتائج التي تم تعلمها من وقوع الحادث الطارئ، ويتم توثيق كل ما يتعلق به للاستفادة من ذلك في المستقبل، ويتم مراجعة خطة التعامل مع الحوادث الطارئة وتقييمها وتصحيح أي عيب فيها أو في المنظومة المعلوماتية لتلافي تكرار هذه الحوادث مستقبلاً.

٤. تقييم المخاطر:

يجب أن تتضمن هذه الخدمة بالحد الأدنى المراحل التالية وذلك وفقاً لمعايير أمن المعلومات التي تقترحها الشركة المعتمدة ويوافق عليها الزبون:

أ. جمع المعلومات عن منظومة الزبون.

ب. تحديد الأصول المعلوماتية لدى الزبون.

ج. تحديد المخاطر التي تواجه هذه الأصول.

د. توصيف الأخطار ودرجة تأثيرها مع ذكر المعيار المستخدم في التوصيف.

هـ. اقتراح الحلول المناسبة لتخفيض هذه الأخطار للمستوى المقبول وفق سياسة أمن المعلومات لدى الزبون.

و. تقديم تقرير مفصل للزبون يتضمن النتائج التي تم التوصل إليها والمقترحات المناسبة.

٥. تقييم الثغرات الامنية:

يجب أن تتضمن هذه الخدمة بالحد الأدنى المراحل التالية وذلك وفقاً لمعايير أمن المعلومات التي تقترحها الشركة المعتمدة ويوافق عليها الزبون:

أ. جمع المعلومات عن منظومة الزبون.

ب. المسح الأمني لاكتشاف الثغرات الأمنية المحتملة.

ج. تحليل وتقييم وتأكيد نتائج المسح الأمني.

د. إعداد التقرير الفني النهائي حول النتائج التي تم التوصل إليها.

٦. اختبار الاختراق:

يجب أن تتضمن هذه الخدمة بالحد الأدنى المراحل التالية وذلك وفقاً لمعايير أمن المعلومات التي تقترحها الشركة المعتمدة ويوافق عليها الزبون:

أ. تحضير أولي مع الزبون.

ب. نمذجة التهديدات.

ج. تحليل الثغرات الأمنية.

د. اختبار إمكانية استغلال هذه الثغرات وفحص قابلية كل ثغرة للحصول على دخول غير شرعي.

هـ. اختبار إمكانية التوسع بالاستغلال للثغرات والاستحواذ على منظومة الزبون.

و. إعداد التقرير الفني النهائي بالنتائج التي تم التوصل إليها.

٧. **استعادة بيانات مفقودة:**

أ. تحديد وسيط التخزين المطلوب استعادة البيانات منه.

ب. تحديد سبب (فقد) ضياع البيانات.

ج. تحديد الأداة المستخدمة لاستعادة البيانات.

د. تنفيذ العمل مع تقديم تقرير مفصل للزبون يتضمن حجم البيانات التي تمت استعادتها والنسبة المئوية للاستعادة.

٨. **مراجعة الكود أمنياً:**

يجب أن تتضمن هذه الخدمة بالحد الأدنى المراحل التالية وذلك وفقاً لمعايير أمن المعلومات التي تقترحها الشركة المعتمدة ويوافق عليها الزبون:

أ. **المرحلة الأولى:** تحضير الملفات التي تحوي الرمازات البرمجية المصدرية، وتجهيز بيئة اختبارية مناسبة للغات البرمجة المستخدمة في تطوير التطبيقات والنصوص البرمجية.

ب. **المرحلة الثانية:** البدء بتدقيق الرمازات المصدرية لتحديد الأخطاء البرمجية أو العيوب أو النواقص التي قد تؤدي إلى وجود ثغرات أمنية قد تؤدي إلى اختراق التطبيق أو فشله بإحدى أو بكلتا الطرق الرئيسية التالية:

١. الفحص اليدوي: ويتم من خلال قراءة النصوص البرمجية وتدقيقها يدوياً.

٢. الفحص باستخدام الأدوات: يتم بواسطة أداة أو مجموعة أدوات متخصصة تصدر تقارير بالنتائج.

ج. **المرحلة الثالثة:** تجهيز تقارير تفصيلية بالنتائج، والتي يجب أن تحوي أسماء الملفات، مكان تواجد الأخطاء البرمجية ضمن الملفات، تفاصيل توضح التأثيرات المحتملة والتي قد تنتج عن هذه الأخطاء، الحلول المقترحة لتصحيح هذه الأخطاء بالإضافة إلى أية تفاصيل أخرى قد تساعد في ضبط وتصحيح هذه الأخطاء.

المادة ٧: حقوق الشركة المعتمدة

أ. تسويق وترويج خدماتها الإلكترونية حسب المادة /٣/ حصراً، وذلك بعد حصولها على الاعتمادية وفقاً للقوانين والأنظمة المعمول بها.

ب. إلغاء أي خدمة من الخدمات المذكورة في شهادة الاعتمادية الممنوحة لها، بموافقة الهيئة.

ج. إضافة خدمة إلى شهادة الاعتمادية الممنوحة لها، بعد الحصول على موافقة الهيئة وتسديد الأجور المطلوبة لذلك.

د. تعديل قائمة الكادر التقني المعني بتقديم الخدمات موضوع الاعتمادية، وذلك بعد موافقة الهيئة للتأكد من استيفائهم للشروط المطلوبة.

هـ. تعديل قائمة الأدوات والبرمجيات المستخدمة من قبلها بعد موافقة الهيئة للتأكد من استيفائها للشروط المطلوبة.

و. تقديم عروض على خدمات أمن المعلومات المقدمة من قبلها وفق الاعتمادية الممنوحة لها، بشرط الحصول على موافقة مسبقة من الهيئة.

المادة ٨: حقوق الزبون

١. تضمن الشركة المعتمدة للزبون الحفاظ على سرية وخصوصية البيانات الخاصة به، وألّا تقوم بإفشائها إلا وفق الأصول والقانون.

٢. الحصول على نسخة ورقية من النتائج التي توصلت لها الشركة المعتمدة و/أو التقارير التي تولدها أدوات الاختبار المستخدمة من قبل الشركة المعتمدة.

٣. الحصول على نسخة إلكترونية من النتائج التي توصلت لها الشركة المعتمدة و/أو التقارير التي تولدها أدوات الاختبار المستخدمة موقعة إلكترونياً من قبل الشركة المعتمدة.

المادة ٩: الرقابة على الاعتمادية

١. تتم الرقابة على التزام الشركات المعتمدة بشروط هذه الوثيقة وفق الآتي:

أ. زيارة دورية كل ستة أشهر للتحقق من التزام الشركة المعتمدة بشروط الاعتمادية الممنوحة لها وإصدار تقرير عن الزيارة.

ب. عند تقديم شكوى من الزبون بالإخلال بأحد شروط الاعتمادية.

٢. يتم توجيه إنذار للشركة المعتمدة في الحالات التالية:

أ. عند ارتكابها مخالفة لأحد بنود هذه الوثيقة.

ب. في حال ثبوت شكوى على الشركة المعتمدة.

٣. تعطى الشركة مهلة خمسة عشر يوماً لتصحيح المخالفة أو معالجة الشكوى، وفي حال لم تصحح الشركة وضعها بعد انقضاء فترة خمسة عشر يوماً من تاريخ تبلغها الإنذار الخطي في موطنها المختار، يتم توجيه إنذار خطي ثانٍ لها وإعطائها مهلة خمسة عشر يوم لاستدراك المخالفة أو الشكوى.

٤. يتم تقييم عمل الشركات المعتمدة قبل ثلاثين يوماً من تاريخ استحقاق تجديد الاعتمادية من كل عام، ويؤخذ بالاعتبار في التقييمات تقرير الرقابة وعدد الإنذارات الموجهة للشركة.

المادة ١٠: تجديد الاعتمادية

١. يتم تجديد الاعتمادية بناء على طلب الشركة على أن يُقدم طلب التجديد قبل خمسة وأربعون يوماً من تاريخ استحقاق التجديد.

٢. يجب أن تسدد الشركة أجور التجديد قبل خمسة عشر يوماً على الأقل من تاريخ استحقاق التجديد.

٣. يتم تجديد الاعتمادية بعد استلام ما يشعر بتسديد أجور التجديد مالم يتم إلغاء الاعتمادية لأحد الأسباب المذكورة في المادة /١١/ من هذه الوثيقة.

٤. يتم نشر قرار تجديد الاعتمادية على الموقع الإلكتروني للهيئة.

المادة ١١: إلغاء الاعتمادية

أ. يحق للهيئة إلغاء الاعتمادية في إحدى الحالات التالية:

١. توقف الشركة المعتمدة عن تقديم خدماتها دون إشعار مسبق للهيئة.

٢. حصول الشركة على إنذارين خلال عام واحد سواءً نتيجة مخالفة أو شكوى، ولم تتم معالجة المخالفة أو الشكوى خلال خمسة عشر يوماً من تاريخ الإنذار الثاني.

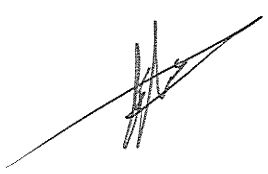
٣. عدم تسديد أجور تجديد الاعتمادية ضمن المهل المحددة.

٤. بناءً على طلب الشركة المعتمدة بعد أن تقوم بتسوية كافة الأمور الإدارية والقانونية والمالية المتعلقة بالاعتمادية.

٥. بناء على قرار قضائي.

ب. يتم نشر قرار إلغاء الاعتمادية على الموقع الإلكتروني للهيئة.

ج. لا يحق للشركة التي ألغي اعتمادها لسبب ما التقدم بطلب جديد إلا بعد مرور عام كامل على الإلغاء.



المادة ١٢: الأجور

أ. تُحدد الأجور عند **منح الاعتمادية للمرة الأولى** وفق جدول الأجور التالي:

الخدمة	استحقاق الدفع	الأجر ل.س
دراسة طلب الاعتمادية	عند تقديم طلب الاعتمادية	١٠٠,٠٠٠
تدقيق أمن نظم المعلومات	قبل الحصول على الاعتمادية	١,٠٠٠,٠٠٠
تطوير سياسة أمن المعلومات	قبل الحصول على الاعتمادية	١,٠٠٠,٠٠٠
وضع خطط التعامل مع الحوادث الطارئة	قبل الحصول على الاعتمادية	٥٠٠,٠٠٠
تقييم المخاطر	قبل الحصول على الاعتمادية	٥٠٠,٠٠٠
تقييم الثغرات الأمنية	قبل الحصول على الاعتمادية	٥٠٠,٠٠٠
اختبار الاختراق	قبل الحصول على الاعتمادية	٥٠٠,٠٠٠
استعادة بيانات مفقودة	قبل الحصول على الاعتمادية	٣٠٠,٠٠٠
مراجعة الكود أمنياً	قبل الحصول على الاعتمادية	٣٠٠,٠٠٠

ب. تُحتسب الأجور عند منح الاعتمادية وفق جدول الأجور وحسب الخدمات التي ستقدمها الشركة.

ج. تُسدّد الشركة المعتمدة الأجور عن كل خدمة ترغب بإضافتها بعد صدور اعتماديتها وفق جدول الأجور.

د. تُسدّد الشركة المعتمدة سنوياً **أجور التجديد** والبالغة ٥٠% (لكل خدمة تقدمها الشركة المعتمدة) من قيمة الأجور المذكورة في جدول الأجور.

هـ. تُعدَّل الأجور الواردة في هذه الوثيقة بقرار من مجلس الإدارة.

الملحق ١
طلب اعتمادية
إلى الهيئة الوطنية لخدمات الشبكة

مقدمه : شركة .....

أرجو الموافقة على منحي شهادة اعتمادية لتقديم خدمات أمن المعلومات التالية:

- ☐ تطوير سياسة أمن المعلومات Security policy Development
- ☐ تدقيق أمن نظم المعلومات Information System Security Auditing
- ☐ وضع خطط التعامل مع الحوادث الطارئة Incident Handling Planning
- ☐ تقييم المخاطر Risk Assessment
- ☐ تقييم الثغرات الأمنية Security Vulnerability Assessment
- ☐ اختبار الاختراق Penetration Testing
- ☐ استعادة بيانات مفقودة Data Recover
- ☐ مراجعة الكود أمنياً Security code review

وتفضلو بقبول الشكر والاحترام

دمشق في / /

العنوان التفصيلي:

معلومات الاتصال:

الاسم والتوقيع والختم

الملحق رقم ٢

الوثائق المطلوبة

١. طلب الحصول على الاعتمادية وفق النموذج المعتمد بالملحق /١/.

٢. سجل تجاري حديث للشركة.

٣. تقرير مفصل عن الأعمال التي قامت الشركة بتنفيذها في مجال خدمات أمن المعلومات لإثبات خبرة الشركة في هذا المجال متضمنة اسم الجهة المستفيدة وتاريخ كل مشروع وزمن الإنجاز.

٤. أسماء الشركات الداعمة (داخلية أو خارجية) إن وجدت.

٥. صورة هوية الشخص طالب الاعتمادية أو المفوض عنه إن وجد.

٦. كتاب من طالب الاعتمادية مصدق أصولاً بالتفويض للشخص المخول بالتوقيع عنه.

٧. قائمة تتضمن أسماء الكادر التقني المعني بتقديم الخدمات موضوع الاعتمادية في الشركة ومؤهلاتهم مع السيرة الذاتية وصورة عن الهوية الشخصية، ووثيقة لا حكم عليه.

٨. إشعار تسديد أجور دراسة طلب الاعتمادية.

٩. تقرير مفصل عن خدمات أمن المعلومات التي ستقدمها الشركة وفق المعايير المعتمدة، على أن يتضمن على سبيل الذكر لا الحصر لكل خدمة التالي: الإجراءات والمراحل، الأدوات البرمجيات التخصصية المستخدمة، المعايير العالمية– إن وجدت– والتي تقدم الخدمة وفقها، أشكال وأنواع الخدمة، مخرجات الخدمة، خبرات فريق العمل.

١٠. تعهد أن البرمجيات المستخدمة ليست منتجاً اسرائيلياً.

١١. تعهد أن الشركة غير محرومة من التعاقد مع الجهات العامة.

١٢. نموذج الاتفاقية التي سيتم تقديم الخدمة من خلالها للزبون (اتفاقية عدم الإفشاء NDA).

١٣. نسخة إلكترونية من الوثائق المطلوبة أعلاه.

الملحق ٣

اختبارات الخدمات

اسم الخدمة	نوع الاختبار
تطوير سياسة أمن المعلومات Security policy Development	عرض تقديمي أمام لجنة مختصة يتضمن: – آلية تقديم الخدمة – المعايير التي يتم تقديم الخدمة وفقها – أعمال سابقة للشركة – قائمة الجهات التي تم تقديم الخدمة لديها – يحق للهيئة التواصل مع الزبائن والتأكد من عدم وجود إشكاليات في تقديم الخدمة.
تدقيق أمن نظم المعلومات Security System Auditing Information	
وضع خطط التعامل مع الحوادث الطارئة Incident Handling Planning	
تقييم المخاطر Risk Assessment	
تقييم الثغرات الأمنية Security Vulnerability Assessment	محاكاة عملية تقديم الخدمة للزبون على بيئة اختبارية في الهيئة في جميع مراحل الخدمة من بداية الخدمة حتى إصدار التقرير النهائي
اختبار الاختراق Penetration Testing	
استعادة بيانات مفقودة Data Recover	
مراجعة الكود أمنياً Security code review	

الملحق٤

خدمات أمن المعلومات المقدمة

اسم الخدمة	الأداة المستخدمة	اسم مقدم الخدمة	معلومات الاتصال لمقدم الخدمة	تاريخ تقديم الخدمة (بدء العقد – انتهاء العقد)	الجهة المستفيدة (الزبون)	ملاحظات (حالة تقديم الخدمة)