



نظام خدمات مركز أمن المعلومات

النسخة الأولى



ضبط اللائحة

سجلات التغيير

التاريخ	إصدار	الحالة	النسخة
		النسخة النهائية	1.0

المراجعات

التاريخ	الاسم	الصفة

المحتويات

٣	الفصل الأول: تعاريف و مصطلحات.....
٣	المادة (١):تعاريف.....
٥	المادة (٢): مصطلحات.....
٦	الفصل الثاني: خدمات المسح الأمني واختبار الاختراق الاحترافية.....
٦	توصيف الخدمات.....
٦	المادة (٣):الهدف من الخدمات.....
٦	المادة (٤):أنواع الخدمات.....
٧	المادة (٥):طرق تقديم الخدمات.....
٧	المادة (٦):مخرجات الخدمات.....
٨	طرق طلب الخدمة.....
٨	المادة (٧):خدمة المسح الأمني العادية.....
٨	المادة (٨):خدمة المسح الأمني الاحترافية وخدمة اختبار الاختراق الاحترافية.....
٩	مراحل المسح الأمني.....
٩	المادة (٩):خدمات المسح العادية للمواقع الإلكترونية.....
٩	المادة (١٠):خدمة المسح الاحترافية.....
١٠	المادة (١١):خدمة اختبار الاختراق الاحترافية.....
١١	المادة (١٢):أجور خدمة المسح و الاختراق.....
١٢	الفصل الثالث: خدمات الاستجابة للطوارئ المعلوماتية SYCERT.....
١٢	المادة (١٣):طرق طلب الخدمة.....
١٢	المادة (١٤):واجبات الزبون.....
١٢	المادة (١٥):مُخرجات الخدمة.....
١٣	المادة (١٦):أجور الاستجابة للطوارئ المعلوماتية.....
١٤	الفصل الرابع: أحكام عامة.....

الفصل الأول: تعاريف و مصطلحات

المادة (١):تعاريف

الهيئة: الهيئة الوطنية لخدمات الشبكة، المحدثة بموجب قانون التوقيع الإلكتروني وخدمات الشبكة رقم /٤/ لعام ٢٠٠٩م.

المركز: مركز أمن المعلومات في الهيئة الوطنية لخدمات الشبكة.

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

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

اختبار الاختراق الاحترافي : خدمة متقدمة تتضمن خدمة المسح الأمني الاحترافي ويضاف إليها اختبار اختراق منظومات الزبون بطرق تحاكي هجوم حقيقي بالتنسيق مع الزبون ، ولا تسبب ضرر لأنظمتها.

جهاز شبكي: جهاز حاسوبي يعمل ضمن الشبكة (موجهات، مبدلات، جدران نارية، أجهزة كشف أو منع الاختراق، الخ).

منظومات معلوماتية: مجموعة منسقة من الأجهزة والبرمجيات الحاسوبية والمعدات الملحقة بها، ومن الأمثلة على المنظومات المعلوماتية: جهاز حاسوبي مع برمجياته المضمنة سواء كانت أساسية أو تطبيقية؛ أو مجموعة من الأجهزة الحاسوبية المترابطة في منظومات موزعة، أو مخدّم تتصل به حواسيب طرفية، أو حاسوب مع المعدات الملحقة به، كالمودم والطابعة والماسح الضوئي، جهاز خلوي الخ.

جهاز حاسوبي: أي جهاز يستخدم التقانات الإلكترونية أو الكهروضوئية أو الرقمية أو أي تقانات

أخرى مشابهة بغرض توليد المعلومات أو جمعها أو حفظها أو الوصول إليها أو معالجتها أو توجيهها أو تبادلها.

الجرائم المعلوماتية: الجرائم المعرفة بقانون تنظيم التّواصل على الشّبكة ومكافحة الجريمة المعلوماتية لعام ٢٠١٢م.

الطوارئ المعلوماتية: هي الحوادث الطارئة التي تؤدي لتهديد أو لتعطل جزئي أو كلي للمنظومات المعلوماتية أو الشبكات أو الخدمات الإلكترونية المقدمة للعاملين أو للمواطنين والتي تقدمها جهات عامة أو خاصة.

الطوارئ الخاصة بالأفراد: الحوادث الطارئة الخاصة بالأفراد والمتعلقة بالجرائم المعلوماتية والتّحليل الجنائي الرّقمي والتي يتم التكليف بمعالجتها أو تحليلها من قبل إدارة الهيئة.

الدليل الرّقمي: البيانات الرّقمية المخزّنة في الأجهزة الحاسوبية أو المنظومات المعلوماتية، أو المنقولة بواسطتها، والتي يمكن استخدامها في إثبات أو نفي جريمة معلوماتية.

السياسة الوطنية لأمن المعلومات واللوائح التنظيمية الملحقة بالسياسة: الوثائق الصادرة عن الهيئة .

الخدمة الاستشارية: خدمة يقدمها المركز تتعلق بتقديم استشارات خاصة بأمن المعلومات وتصميم الشبكات وتطوير المنظومات المعلوماتية والخدمات الإلكترونية الأمانة.

الزّيون: قطاع عام أو قطاع خاص أو أفراد.

طلب الخدمة: وثيقة إلكترونية أو ورقية تتضمن المعلومات الأساسية الواجب تقديمها للبدء بالخدمة.



المادة (٢): مصطلحات

المصطلح باللغة الانكليزية	المصطلح باللغة العربية
Security Vulnerability Scanning	المسح الأمني
Penetration Testing	اختبار الاختراق الاحترافي
Information Systems	منظومات معلوماتية
computer device	جهاز حاسوبي
Elimination of false positive	عملية التحقق من الوجود الحقيقي للثغرات
System backup	نسخ احتياطي
Information gathering	جمع معلومات
Web vulnerability Scanning	خدمة المسح الأمني الاحترافية للمواقع ومخدمات الويب
Application Vulnerability Scanning	خدمة المسح الأمني الاحترافية للبرمجيات
Network Vulnerability Scanning	خدمة المسح الأمني الاحترافية للشبكات

الفصل الثاني: خدمات المسح الأمني واختبار الاختراق الاحترافية

توصيف الخدمات

المادة (٣): الهدف من الخدمات

رفع مستوى الأمان ضد الهجمات الإلكترونية ومحاولات الاختراق، من خلال كشف الثغرات الأمنية المعلوماتية الموجودة لدى الزبون والتي يمكن استغلالها من قبل المهاجمين وقرصنة المعلوماتية، ويتم ذلك بالاعتماد على مجموعة من أفضل البرامج والتجهيزات الاحترافية المرخصة من أفضل الشركات العالمية، بالإضافة إلى تقديم أفضل الحلول الممكنة لمعالجة هذه الثغرات.

المادة (٤): أنواع الخدمات

١. خدمة المسح الأمني العادية: يقدم المركز هذه الخدمة عند الطلب لجميع المواقع الإلكترونية العامة والخاصة، وهي مجاناً للجهات العامة ولمرة واحدة خلال العام.
٢. خدمة المسح الأمني الاحترافية: يقدم المركز هذه الخدمة عند الطلب للجهات العامة والخاصة، وتقسم إلى ثلاثة أنواع:

- أ. خدمة المسح الأمني الاحترافية للمواقع ومخدمات الويب.
- ب. خدمة المسح الأمني الاحترافية للبرمجيات.
- ت. خدمة المسح الأمني الاحترافية للشبكات.

٣. خدمة اختبار الاختراق الاحترافية: تتضمن خدمة المسح الأمني الاحترافية السابقة، ويضاف إليها اختبار

اختراق منظومة الزبون بطرق تحاكي هجوم حقيقي بالتنسيق مع الزبون.

المادة (٥): طرق تقديم الخدمات

يتم تقديم الخدمة بإحدى الطرق التالية، ويعود لإدارة المركز تقدير ذلك بالاتفاق مع الزبون بحسب ما تتطلبه ظروف المسح:

١. المسح الأمني عن بعد من خلال المركز.
٢. المسح الأمني بموقع العمل من خلال زيارة فريق متخصص من المركز للزبون.
٣. المسح الأمني بموقع العمل وعن بعد بحسب متطلبات العمل.

المادة (٦): مخرجات الخدمات

يحصل الزبون على تقرير تفصيلي، يتضمن مايلي:

١. جميع المعلومات التي تم الحصول عليها من خلال المسح الأمني، مثل: منظومات التشغيل المستخدمة، والتقنيات والبرمجيات المستخدمة وإصداراتها، والخدمات الإلكترونية والبوابات المفتوحة والعناوين الشبكية (IPs) وغيرها.
٢. الثغرات الأمنية المكتشفة، ودرجة خطورتها، وتأثيرها على العمل.
٣. الحلول المقترحة لمعالجة الثغرات الأمنية.
٤. أية معلومات تُفيد الزبون في تحسين واقع أمن المعلومات لديه.

طرق طلب الخدمة

المادة (٧): خدمة المسح الأمني العادية

١. تقدم الخدمة مجاناً للجهات العامة مرة واحدة في العام، ودون طلب من الزبون .
٢. تُقدم الخدمة بناءً على طلب مباشر من الزبون أو من مزود خدمة الاستضافة، أو من خلال ملء طلب الخدمة المُتوفر على الموقع الإلكتروني للهيئة أو للمركز، وإرساله إلكترونياً، أو عن طريق الفاكس.
٣. يلتزم الزبون بتقديم إشعار، يُفيد تسديده لرسوم الخدمة عند ملء الاستمارة المطلوبة.

المادة (٨): خدمة المسح الأمني الاحترافية وخدمة اختبار الاختراق الاحترافية

١. تُقدم الخدمة من خلال ملء طلب الخدمة المُتوفر على الموقع الإلكتروني للهيئة أو للمركز، وإرساله إلكترونياً، أو عن طريق الفاكس.
٢. يقوم المركز بدراسة الطلب وإعداد العقد اللازم.
٣. توقيع العقد من كلا الطرفين.
٤. واجبات الزبون:

- تقديم كافة المعلومات والبيانات التي يطلبها المركز والتي تُمكنه من تقديم الخدمة بالشكل الأمثل.
- تحضير بيئة العمل للمسح الأمني وفق ما يطلبه المركز، والوارد بالعقد مثل:
 - أ. نسخ احتياطي للمنظومات المعلوماتية التي سيتم مسحها.
 - ب. السماح لبرمجيات المركز بالوصول إلى المنظومات المعلوماتية المُستهدفة عبر تجهيزات الحماية إن وجدت، وذلك في حال تم المسح عن بعد.

ت. إنشاء حساب مؤقت خاص بعملية المسح وبصلاحية مدير على المنظومات المعلوماتية التي

سيتم مسحها.

ث. إلغاء جميع السماحيات والإجراءات والحسابات المنشأة لغرض المسح بعد الانتهاء التام من

المسح الأمني.

مراحل المسح الأمني

المادة (٩): خدمات المسح العادية للمواقع الإلكترونية

١. يتم المسح من خلال برمجيات احترافية لدى المركز.
٢. إعداد تقرير بالنتائج التي تم الحصول عليها.
٣. إرسال التقرير للزبون من خلال البريد الرسمي والإلكتروني.

المادة (١٠): خدمة المسح الاحترافية

يتم المسح من خلال برمجيات احترافية لدى المركز وفق المراحل التالية:

١. جمع المعلومات عن المنظومات المراد مسحها.
٢. المسح الأمني للمنظومات.
٣. تحليل الثغرات المكتشفة من خلال عملية المسح وفق خطورتها وتأثيرها.
٤. اختبار كل ثغرة على حدى، بحسب درجة الخطورة والتحقق من وجودها الفعلي.
٥. إعداد تقرير تفصيلي يتضمن مايلي:

أ. الهدف من المسح.

ب. الثغرات المكتشفة لدى الزبون ونوعها ودرجة خطورتها وتأثيرها.

ت. الحلول المقترحة والجهة المسؤولة عن تنفيذها.

ث. نصائح ومعلومات هامة للزبون مثل مخطط الأجهزة والخدمات وغيرها.

٦. تقديم التقرير للزبون ومناقشته معه.

المادة (١١): خدمة اختبار الاختراق الاحترافية

يتم المسح واختبار الاختراق الاحترافي من خلال برمجيات احترافية لدى المركز وفق المراحل التالية:

١. جمع المعلومات عن المنظومات المراد اختبارها.
٢. المسح الأمني.
٣. تحليل الثغرات المكتشفة من خلال عملية المسح وفق خطورتها وتأثيرها.
٤. اختبار كل ثغرة على حدى بحسب درجة الخطورة والتحقق من وجودها الفعلي.
٥. تحضير الأدوات والبرمجيات المناسبة للاختراق الاحترافي.
٦. التعاون مع الزبون، لإعلامه ببدء اختبار الاختراق الاحترافي والإجراءات الواجب اتخاذها من قبله.
٧. إجراء الاختراق الاحترافي.

٨. إعداد تقرير تفصيلي يتضمن مايلي:

أ. الهدف من الاختراق.

ب. الخطوات المتبعة في الخدمة.

ت. مخططات البنية التحتية العاملة لدى الزبون .

ث. الثغرات المُكتشفة لدى الزّيون ونوعها ودرجة خطورتها وتأثيرها.

ج. الحلول المقترحة والجهة المسؤولة عن تنفيذها.

ح. نصائح ومعلومات هامة للزّيون.

٩. تقديم التقرير للزّيون ومناقشته معه.

المادة (١٢): أجور خدمة المسح و الاختراق

ملاحظات	الأجر		الخدمة
تقدم الخدمة مجاناً للجهات العامة مرة واحدة في العام	10,000 (ل.س)		خدمة المسح العادية
في حال خدمة مسح البرمجيات أو الشبكات يضاف عن كل مخدم 10,000 ل.س وعن كل جهاز شبكي 2,000 ل.س 25,000 عن كل شبكة محلية (LAN)	75,000	للمواقع الإلكترونية	خدمة المسح الاحترافية
	125,000	لمخدمات الويب والبرمجيات	
	250,000	للشبكات	
في حال خدمة الاختراق للبرمجيات أو للشبكات يضاف عن كل مخدم يخضع للاختبار 20,000 ل.س وعن كل جهاز حاسوبي يخضع للاختبار 5,000 ل.س	100,000	للمواقع الإلكترونية	خدمة اختبار الاختراق الاحترافي
	200,000	لمخدمات الويب والبرمجيات	
	300,000	للشبكات	

الفصل الثالث: خدمات الاستجابة للطوارئ المعلوماتية SYCERT

المادة (١٣): طرق طلب الخدمة

يمكن للزبون التّقدم بطلب الخدمة بإحدى الطّرق التّالية:

١. طلب خطي للهيئة من قبل الزّبون يُوضح الحادثة التي يطلب الاستجابة لها.
٢. الاتصال الهاتفي بالمركز بحيث يقوم الموظفون المكلفون بتلقي الطلبات بتعبئة طلب الخدمة والتي يمكن توقيعها لاحقاً من الزّبون.
٣. ملء طلب الخدمة المتوفر على الموقع الإلكتروني للهيئة أو للمركز وإرساله عن طريق البريد الإلكتروني أو عن طريق الفاكس.

المادة (١٤): واجبات الزّبون

١. تقديم كافة المعلومات والبيانات التي يطلبها المركز والتي تمكّنه من الاستجابة للحادثة.
٢. السماح لعناصر المركز بالوصول للملفات والتجهيزات المتعلقة بالحادثة.

المادة (١٥): مُخرجات الخدمة

تقرير مُفصل من قبل المركز يتضمن تفاصيل الحادثة والحلول الإسعافية (الآنية) والاحترازية (المستقبلية) المقترحة.

المادة (١٦): أجور الاستجابة للطوارئ المعلوماتية

١. الخدمة مجانية للجهات الحكومية.

٢. تحدد الأجور للأفراد والجهات الخاصة كما يلي:

ملاحظات	الأجر حسب سعة التخزين			الخدمة
	الأجر (ل.س.)	إلى GB	من GB	
يقصد بالبيانات المفقودة: ملفات إلكترونية بكافة أنواعها، منظومات تشغيل، تطبيقات وغيرها من البيانات المخزنة إلكترونياً.	2,000	٦٤	--	استعادة بيانات أو معلومات مفقودة (Data Recovery)
	5,000	٥٠٠	٦٤	
	7,000	1,000	٥٠٠	
	7,000 لكل 1TB	ما فوق	1,000	
كل جهاز حاسوبي يقوم فريق المركز بفحصه.	10,000 ل.س لكل جهاز حاسوبي.			طوارئ معلوماتية
	10,000 ل.س للأفراد عن كل جهاز، 20,000 ل.س عن كل جهاز للجهات الخاصة.			استخراج الدليل الرقمي لجريمة معلوماتية أو تقليدية

الفصل الرابع: أحكام عامة

١. يمكن لإدارة الهيئة تخفيض الأجر الواردة في هذا النظام لبعض الجهات وفق ما تقتضيه المصلحة

العامة، وذلك بموافقة من مجلس إدارة الهيئة.

٢. تخفض أجر الخدمات المقدمة للقطاع العام بنسبة ٢٠ % عن الأجر الواردة في هذه الوثيقة.

٣. يتم تسديد الأجر لحساب الهيئة في المصرف التجاري السوري، كما يلي:

أ. خدمة المسح الأمني العادية، يجب تسديد كامل الأجر قبل البدء بالخدمة.

ب. خدمات الاستجابة للطوارئ المعلوماتية، يسدد ١٠% من الأجر قبل البدء بالخدمة ويتم تسديد

باقي الأجر في حال الوصول لنتيجة وقبل تسليم التقرير النهائي ويستثنى من هذا البند خدمة

طوارئ المعلوماتية .

ت. باقي الخدمات، يجب على الزبون تسديد ٥٠% من قيمة الأجر عند مباشرة المركز بتقديم

الخدمة، على أن يتم تسديد باقي الأجر عند انتهاء المركز من تقديم الخدمة بالكامل بحسب

بنود العقد مع الزبون .

٤. جميع المعلومات الخاصة بالزبون بما في ذلك نتائج الاختبارات هي معلومات سرية ويحق للمركز

استخدامها لغرض إجراء الدراسات الإحصائية لتقييم واقع أمن المعلومات في سورية فقط.