



الهيئة الوطنية لخدمات الشبكة  
National Agency For Network Services

الجمهورية العربية السورية

وزارة الاتصالات والتقانة

الهيئة الوطنية لخدمات الشبكة

### دفتر الشروط الفنية

لتوريد وتركيب وإعداد واختبار وتشغيل

مشروع الاستجابة للطوارئ المعلوماتية بمركز أمن المعلومات

في الهيئة الوطنية لخدمات الشبكة

التصنيف: عادي

ديوان الهيئة الوطنية لخدمات الشبكة	
الرقم	٢٥٢ / ١٤
الواردة	٣ / ٢٠٢٠ م




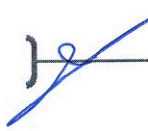

2020

{ 1 }

## 1. المحتويات

### Table of Contents

المحتويات	1
.....	2
مقدمة	2
.....	3
تعريف	2.1
.....	4
نظرة عامة عن المشروع	3
.....	4
الموقع	3.1
.....	4
أهداف المشروع	3.2
.....	4
نقاط التواصل	3.3
.....	5
ملخص الأعمال العقدية	3.4
.....	5
أسس قياس نجاح المشروع	3.5
.....	6
الشروط العامة	4
.....	6
رفض العرض الفني:	5
.....	8
تنفيذ المشروع:	6
.....	9
مركز أمن المعلومات (المركز)	7
.....	9

   { 2 }  

المكونات الحالية للمخبر الوطني لأمن المعلومات.....	7.1
.....	10
توصيف متطلبات التركيب لمكونات المشروع.....	8
.....	11
الشروط والمواصفات الفنية: .....	9
.....	12
متطلبات أخرى.....	9.1
.....	17
اختبار المشروع.....	10
.....	19
التدريب .....	12
.....	20
الوثائق .....	13
.....	21

## 2. مقدمة

أ. تقوم الهيئة الوطنية لخدمات الشبكة عبر مركز أمن المعلومات بـ:

1. وضع المواصفات والمعايير الخاصة بأمن وحماية الشبكات ومواقع الإنترنت، والإشراف على حسن الالتزام بها.

2. وضع المعايير الخاصة بمواجهة حالات الطوارئ على الإنترنت أو غيرها من الشبكات المعلوماتية والحاسوبية، والإشراف على حسن الالتزام بها؛ وتأليف فرق عمل للتصدي لهذه الحالات.

3. يعد هذا المشروع، مشروع وطني يعمل على تعزيز وتنفيذ مهام فريق الاستجابة للطوارئ المعلوماتية في الجمهورية العربية السورية.

## 2.1. تعاريف

- أ. إضافة إلى التعاريف الواردة في قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية الصادر بالقانون رقم 17/ لعام 2012 والسياسة الوطنية لأمن المعلومات واللوائح التنظيمية لها لعام 2014. يُقصد بالتعابير التالية، في معرض هذه الوثيقة، المعنى المبين إلى جانب كل منها:
- الإدارة: الهيئة الوطنية لخدمات الشبكة المحدثة بالقانون رقم 4/ لعام 2009.
  - مركز أمن المعلومات /المركز/: المركز المسؤول عن أمن المعلومات على المستوى الوطني.
  - مركز الاستجابة للطوارئ المعلوماتية /المشروع/: المركز المسؤول عن تقديم الدعم والمساعدة لجميع مستخدمي الشبكات المعلوماتية والإنترنت والأنظمة المعلوماتية بكل ما يتصل بالحوادث والمخاطر المعلوماتية.
  - منظومة معلوماتية: مجموعة متسقة من الأجهزة والبرمجيات الحاسوبية والمعدات الملحقة بها.
  - الخطر المعلوماتي: احتمال أن يستغل مصدر تهديد محدد (يحدث بشكلٍ عرضي أو بشكل مقصود) نقطة ضعف محددة في نظام المعلومات.
  - إدارة المخاطر: العملية الكلية لتحديد ومراقبة المخاطر ذات الصلة بأنظمة المعلومات والحد من آثارها.
  - تعني كلمة "يجب" أو "مطلوب" المستخدمة في هذه الوثيقة أن البند مطلوب حتماً للمواصفات.
  - تعني كلمة "يجوز" أو "اختياري" المستخدمة في هذه الوثيقة أن البند اختياري.
  - تشير كلمة "بلد" إلى "الجمهورية العربية السورية".

## 3. نظرة عامة عن المشروع

### 3.1 الموقع

- أ. مركز أمن المعلومات، مبنى الإدارة، تقاطع صحارى، ريف دمشق.

### 3.2 أهداف المشروع

- أ. إنشاء مركز تنسيق على المستوى الوطني و/أو على المستوى الإقليمي بشكل مركزي، بهدف التنسيق للتعامل مع الحوادث المعلوماتية الطارئة. (مع إمكانية الربط مستقبلاً مع مراكز استجابة للطوارئ المعلوماتية بالبلد).
- ب. بناء فريق استجابة للطوارئ المعلوماتية يتمتع بالمؤهلات والخبرات المناسبة ومتابعة تدريب وتأهيل أعضاء الفريق بشكل مستمر، وتتبع التطورات في مجال أمن المعلومات.
- ج. وضع وتطوير معايير خاصة بالاستجابة للحوادث المعلوماتية الطارئة.
- د. وضع وتطوير السياسات الأمنية الوطنية في هذا المشروع والإشراف على الالتزام بها.



- هـ. تطوير بنية لتنسيق الاستجابة للحوادث المعلوماتية الطارئة على المستوى الوطني وتحديد زمن الاستجابة لها.
- و. تطوير القدرة على دعم الإبلاغ عن الحوادث عبر مجموعة واسعة من الطرق والأساليب بما يضمن السرعة والدقة.
- ز. إدارة الحوادث ونقاط الضعف والثغرات والتهديدات ودراسة وتحليل كل ذلك وتوثيق النتائج.
- ح. إجراء الدراسات والأبحاث وتطوير الخبرات المعرفية في مجال الأمن المعلوماتي وذلك على المستوى الوطني.
- ط. دعم ومساعدة الجهات داخل البلد على تطوير قدراتها الخاصة في إدارة الحوادث المعلوماتية.
- ي. نشر التوعية وثقافة أمن المعلومات باستخدام كافة الوسائط المتاحة، كتوفير توجيهات عامة لتأمين الشبكات والتجهيزات والموارد الأخرى.
- ك. تطوير مواد التدريب والتوعية بأنواعها وبكافة مستويات المستخدمين المستهدفين من المستخدم الفرد العادي إلى مدراء ومشرقي المعلوماتية في الجهات.

### 3.3 نقاط التواصل

أ. للاتصال مع الإدارة في الأمور الفنية: مركز أمن المعلومات

1. البريد الإلكتروني: infosec@nans.gov.sy

2. الهاتف: +963 11 3937047

3. الفاكس: +963 11 3937079

4. العنوان البريدي: دمشق - الصبورة - 60.

ب. تؤمن نقطة الاتصال الإجابة على الأسئلة المتعلقة بهذا الدفتر الفني.

### 3.4 ملخص الأعمال العقدية

أ. إنشاء مركز العمليات الأمنية (SOC) القادر على استيعاب معالجة وتحليل الحوادث المعلوماتية المتعلقة بالإدارة، بحيث تشمل ما يلي:

1. مركز المعطيات الوطني.

2. الشبكة الحكومية الآمنة.

3. منظومة المدفوعات الإلكترونية.

ب. تقديم تصميم مفصل (متضمناً مواصفات جميع تجهيزات وبرمجيات المشروع) كجزء من اقتراح العارض للأنظمة المقترحة والمطلوبة وذلك لتشغيل المشروع.

ج. توريد وتسليم وتركيب وإعداد ومعايرة واختبار جميع التجهيزات والبرمجيات موضوع التعهد بما فيها اتصالات الشبكة اللازمة للمشروع.

- د. توريد وتسليم وتركيب جميع البرمجيات وتطبيقات المنظومة مع التراخيص اللازمة ذات الصلة في حال وجودها.
- هـ. يجب على العارض تقديم خطة اختبار عمل المشروع في عرضه الفني للتحقق من عمل كافة التجهيزات والبرمجيات والمنظومات موضوع العقد بالشكل الأمثل ويجب أن تحصل على موافقة الإدارة.
- و. تقديم المواصفات والمزايا الفنية لجميع مكونات المشروع المقترح بالتفصيل ومع الرسوم البيانية والتصاميم.
- ز. تقديم خطة للتدريب، وإجراء التدريب لكوادر الإدارة على إدارة المشروع والعمليات، والصيانة كجزء من خطة التدريب الموضحة في قسم التدريب، وتنظيم عملية نقل المعرفة اللازمة أثناء فترة التشغيل.
- ح. توفير مجموعة كاملة من وثائق المشروع.
- ط. يجب أن ينهي المتعهد كافة عمليات التوريد والتركيب والاختبار والتدريب والتشغيل وغيرها من الأعمال المذكورة في هذه الوثيقة خلال فترة التنفيذ البالغة /240/ يوم اعتباراً من أمر المباشرة متضمنة أيام العطل الرسمية والأعياد والمناسبات الوطنية.

### 3.5 أسس قياس نجاح المشروع

- أ. استقرار عمل المشروع من خلال سرعة معالجة المشاكل بشكل تام من قبل العارض وعدم تكرارها، وألا تؤثر على عمل المشروع سواء على مستوى البرمجيات أو التجهيزات أو منظومات الاتصال خلال مدة 3 أشهر من بدء التشغيل.
- ب. يجب ألا تواجه الإدارة أي مشاكل بالأداء حتى مع حمل يزيد عن 60% على كامل المشروع أو أحد مكوناته.
- ج. يجب أن يكون المشروع مصمم ومنفذ ومخصص بسهولة وبعيد عن التعقيد.
- د. يجب أن يدعم المشروع توزيع الحمل على أكثر من تجهيزة لزيادة التوافرية والأداء.
- هـ. خلو المشروع من نقاط الفشل المفردة.

### 4. الشروط العامة

- أ. يقدم العارض نسختين من العرض الفني (ورقية + إلكترونية).
- ب. يجب على العارض تقديم لمحة عن شركته، وبيان مدى خبرة الشركة بمجال أمن المعلومات. وبيان المشاريع المنفذة في مجال أمن المعلومات وتحديداً بمجال بناء مراكز الاستجابة للطوارئ المعلوماتية.
- ج. يعتبر هذا المشروع متكامل/تسليم مفتاح باليد (Turn Key Solution) لذلك يجب على العارض أن يلبي كافة المتطلبات لضمان نجاح المشروع حتى لو لم يتم ذكرها في دفتر الشروط هذا.
- د. يجب على العارض تقديم لمحة عن تاريخ الشركات المنتجة للتجهيزات والبرمجيات وملاءمتها الفنية والمالية.

- هـ. يجب أن تكون التجهيزات والبرمجيات المقدمة من تصنيع شركات متخصصة وذات سمعة جيدة في هذا المجال، وأن تكون جديدة وغير مجددة، ومن أحدث الطرازات المنتجة بحلول تقديم العرض الفني.
- و. يجب أن يكون العرض المقدم للمشروع من قبل العارض مرناً وقابل للتوسع عند الطلب.
- ز. يجب أن يكون الحل المقدم من قبل العارض معيارياً وقابلًا للتطوير ويمكن ترقيته بمرونة، كما يجب أن يقدم العارض وصف مفصل حول هذه الميزات والحدود القصوى لعمل المشروع وفق الحل المقدم من قبله جنباً إلى جنب مع المتطلبات التفصيلية لتوسيع السعة إلى الحد الأقصى المذكور دون الحاجة إلى تغيير العناصر الأساسية للمشروع أو استبدال الأجهزة الأساسية.
- ح. تم إعداد هذا الدفتر بعناية وذلك بعدم ترك أي غموض في الأعمال المطلوبة. في حال فشل العارض في فهمه أو أنه يحتاج إلى أي توضيح، يجب أن يتواصل مع الإدارة بموجب كتاب خطي. لا يُسمح بالافتراضات ما لم يذكر بوضوح ويعد مقبولاً من قبل الإدارة.
- ط. يجب على العارض زيارة موقع العمل قبل تقديم عرضه الفني للوقوف على واقع عمل المركز وأي متطلبات أخرى يراها العارض ضرورية لتقديم عرضه الفني.
- ي. يجب على العارض مراعاة موجودات مركز أمن المعلومات والمذكورة لاحقاً ودمجها في الحل المقدم من قبله بحيث يتم استثمارها في المشروع بالشكل الأمثل.
- ك. يجب على العارض تقديم إجابة كاملة ومفصلة عن هذا الدفتر بنداً بنداً في عرضه الفني، والذي يشمل:
- وصف مفصل.
  - إقرار بالامتثال بنداً بنداً مع جميع البنود والشروط ومتطلبات هذا الدفتر.
  - الوصف الفني التفصيلي ومواصفات المنظومات المقترحة وغيرها من الوثائق اللازمة لدعم إقرار الامتثال.
- ل. يجب على العارض أن يقدم جميع المعلومات عن مكونات المشروع والتي تحتوي على العلامة التجارية والطراز والنسخة، وبلد التصنيع وشركة التصنيع وعام التصنيع.
- م. تفضل التراخيص الدائمة على التراخيص السنوية، وستحدد الإدارة الاختيار المناسب، ويجب على العارض أن يقدم بعرضه قائمة مفصلة بجميع تراخيص المنتجات.
- ن. يجب على العارض أن يقدم عرضاً لتجديد التراخيص للبرمجيات والتجهيزات التي يتطلب عملها رخص نظامية وذلك للأعوام الخمسة القادمة، ويجب أن يلتزم العارض بهذا العرض، وسوف تنظر الإدارة في هذا العرض ولكنها غير ملزمة به، يجب أن يتضمن العرض وصفاً مفصلاً حول الآثار الجانبية التي قد تحدث في المشروع في حالة انتهاء صلاحية ترخيص واحد أو أكثر وعدم إعادة تنشيطه.



س. يجب أن يحدد العارض بوضوح أي ميزات ذات قيمة مضافة غير مذكورة في دفتر الشروط هذا وفوائد هذه الميزات وستؤخذ الميزات الإضافية بعين الاعتبار عند إجراء التقييم الفني.

ع. يجب على العارض أن يصف بالتفصيل استقرار الحل وتوافره والذي يجب ألا يقل عن 99.999٪.

ف. يجب أن تدعم البرمجيات والتجهيزات الشبكية المقدمة بروتوكول العنوان الإصدار السادس IPV6 بالإضافة إلى العنوان الإصدار الرابع.

ص. يجب تقديم تصميم أولي وتفصيلي في العرض الفني يتضمن على سبيل الذكر لا الحصر:

1. بنية النظام (مكونات المشروع).

2. تحديد مستوى التكرارية المطبقة (التجهيزات والبرامج) مع الأخذ بعين الاعتبار ما يلي:

i. لا يتم قبول نقطة فشل واحدة في أي جزء من المشروع.

ii. يجب ألا يؤثر الفشل في أي عقدة مفردة على الأداء العام والعدد الإجمالي للجلسات

المتزامنة المدعومة في النظام.

ق. في حالة التحديث و/ أو التحسين، حيث تصبح الإصدارات الجديدة من البرمجيات متاحة قبل شحن المنتجات؛ وفي حالة رغبة العارض بتوفيره يجب إبلاغ الإدارة بذلك بحيث تكون الإصدارات الجديدة لها نفس المواصفات الفنية أو أفضل من المواصفات المتعاقد عليها وذلك دون تعديل السعر، ويكون التحديث مشروط بموافقة الإدارة.

ر. يجب على المتعهد الالتزام بتقديم الدعم الفني خلال فترة الضمان المجاني وبزمن استجابة لا يتجاوز ثلاث ساعات من إعلامه عن طريق الهاتف أو الفاكس أو البريد الإلكتروني أو عبر كتاب رسمي، كما يطلب من المتعهد معالجة المشاكل وتصحيح الأخطاء، واستبدال التجهيزات أو البرمجيات التي قد يطرأ على عملها أي عطل بأخرى جديدة بنفس المواصفات أو مواصفات أعلى، على أن تخضع لفترة ضمان جديدة.

ش. لا يتقاضى المتعهد أي أجور لقاء تقديمه للبرمجيات المجانية أو المفتوحة المصدر المتاحة للجميع على شبكة الإنترنت والتي قد تدخل في بنية المشروع، ويمكن أن يتقاضى الأجور اللازمة لتنصيبها وإعدادها لتعمل بالشكل الأمثل.

ت. يضمن العارض أن جميع مكونات المشروع من تجهيزات وبرمجيات تعمل بشكل جيد ويتم تحديثها بشكل صحيح وطبيعي وبدون أي مشاكل داخل البلد.

ث. يلتزم العارض بتوقيع اتفاقية عدم إفشاء المعلومات مع الإدارة تشمل كافة المعلومات المتعلقة ببيئة العمل والمشروع.

5. رفض العرض الفني:

أ. يعتبر العرض مرفوض فنياً في الحالات التالية:



1. عدم اطلاع العارض على موقع العمل والأعمال الواجب إنجازها ومواصفات التجهيزات والبرمجيات الموجودة مسبقاً في المركز قبل تقديم العروض الفنية والمالية وتقديم تصريح يثبت ذلك.
2. وجود تحفظ على أي من بنود دفاتر الشروط الفنية والحقوقية والمالية.
3. تقديم العارض لجزء من الكميات المطلوبة دون تقديم الكميات الأخرى.
4. تقديم العارض لتجهيزات مجددة أو غير جديدة أو مجموعة محلياً.
5. تقديم تجهيزات أو برمجيات برخص غير نظامية أو مقرصنة.
6. توقف عمل المشروع بانتهاء صلاحية التراخيص.
7. وجود نقطة فشل مفردة تؤدي إلى توقف عمل المشروع.

#### 6. تنفيذ المشروع:

##### ينفذ المشروع على مرحلتين:

- المرحلة الأولى: ومدتها /150/ يوم، وتتضمن تنفيذ كافة أعمال التوريد والتركيب والتنصيب والإعداد والاختبار والتدريب، وتبدأ من اليوم التالي لتاريخ تبليغ المتعهد أمر المباشرة.
- المرحلة الثانية: وهي مرحلة التشغيل ومدتها /90/ يوم، وتتضمن تنفيذ كافة أعمال التشغيل وتبدأ اعتباراً من اليوم التالي بتاريخ إعلام المتعهد بمصادقة الإدارة على محضر الاستلام المؤقت للمرحلة الأولى.

#### 7. مركز أمن المعلومات (المركز)

- أ. يمثل المركز الوحدة التنظيمية المسؤولة عن وضع المواصفات والمعايير وكافة الوثائق الخاصة بأمن وحماية المعلومات والشبكات بما فيها المواقع الإلكترونية على الشبكة والإشراف على حسن الالتزام بها. وإنجاز الأبحاث والاختبارات اللازمة والممكنة في إطار تأمين بيئة عمل مناسبة وأمنة. ووضع المعايير الخاصة بمواجهة حالات الطوارئ على الشبكة أو غيرها من الشبكات المعلوماتية واتخاذ ما يمكن من إجراءات وقائية وعلاجية، وإدارة فرق عمل للتصدي لها.
- ب. يمارس المركز مهامه من خلال الدوائر التالية:
  1. دائرة أمن الشبكات والنظم الحاسوبية.
  2. دائرة الدراسات والأبحاث.
  3. دائرة الاستجابة للطوارئ المعلوماتية.
- ج. ولكي يقوم المركز بتنفيذ المهام الموكلة إليه تم تأسيس منظومة خاصة بالسبر الأمني واختبار الاختراق "المخبر الوطني لأمن المعلومات".

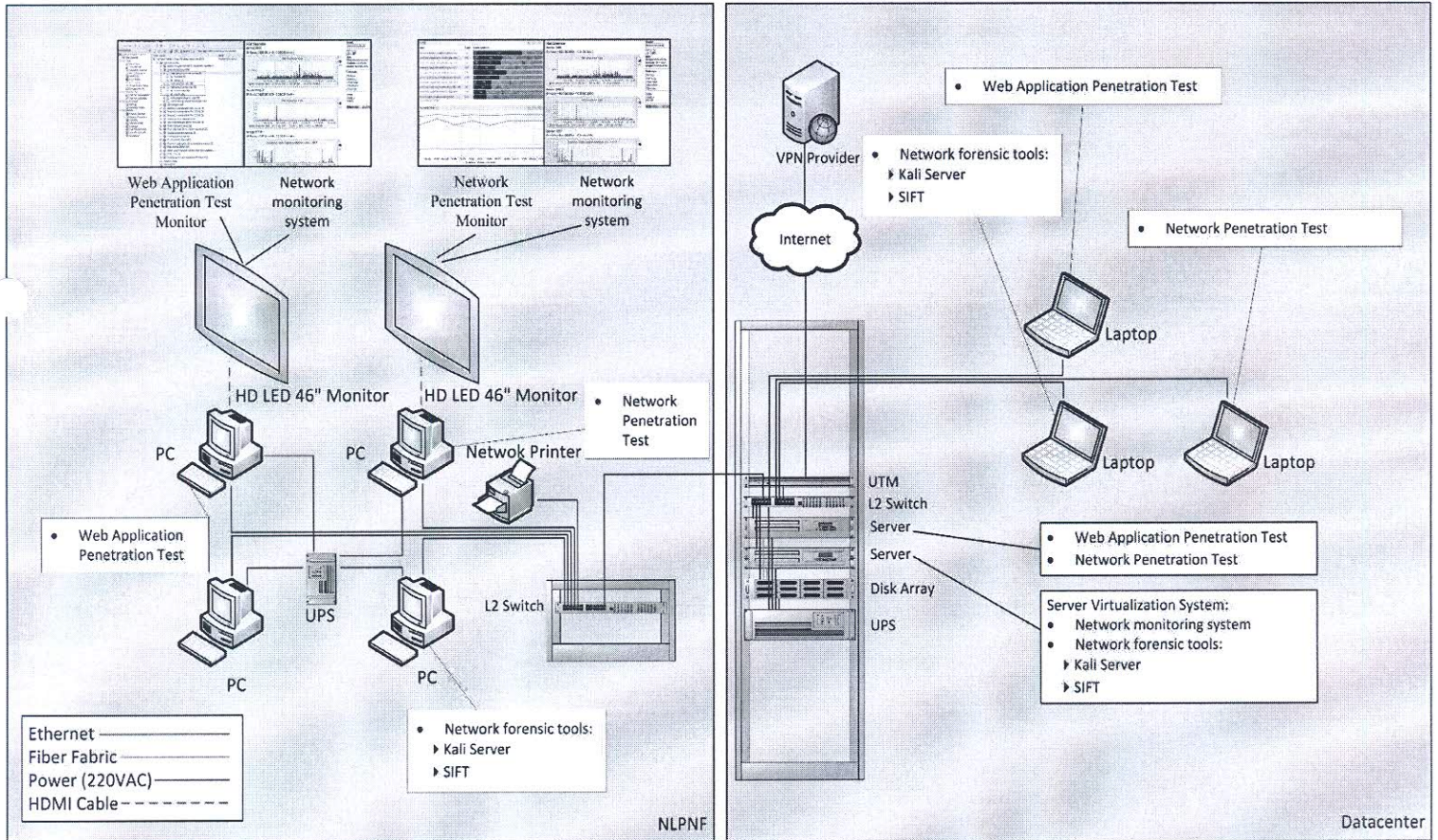
## 7.1 المكونات الحالية للمخبر الوطني لأمن المعلومات

أ. إن الغاية من هذا البند تعريف العارض بمكونات المخبر بحيث يتم دمجها واستثمارها في الحل الفني المقدم من قبله وهي:

الوظيفة	العدد	برمجيات وتطبيقات
برنامج مسح الشبكات والنظم	1	Tenable Nessus 7 Professional
برنامج مسح تطبيقات الويب	3	Acunetix 9.5 Web Vulnerability Scanner
اختبار الاختراق / مسح - مفتوح المصدر	2	KALI Advanced Penetration Testing OS
500 Gb: تم استهلاك معظم الحزمة	1	VPN Subscription
تحليل جنائي رقمي، استعادة البيانات - مفتوح المصدر	1	CAIN+SIFT (Data recovery +Forensic)
معلومات إضافية	العدد	تجهيزات
أنظمة تشغيل windows pro 2008 عدد 2	4	مخدم مركزي
مع أنظمة تشغيل Windows 10 مرخصة	4	محطات عمل وحواسب مكتبية
3 مع أنظمة تشغيل مرخصة 2 بدون أنظمة تشغيل	5	حواسب محمولة
-	2	شاشات مراقبة جدارية
UTM	1	وحدة حماية مركزية
-	1	KVM
Gateway	1	موجه
Fiber 20 Mbps	1	خط اتصال إنترنت
ADSL 2 Mbps	1	خط اتصال إنترنت
مستقلة فيزيائياً عن شبكة الإدارة	1	شبكة داخلية كاملة



10KVA, 5KVA	2	وحدة عدم انقطاع التيار الكهربائي
Huawei	2	مبدلة شبكية L3



## 8. توصيف متطلبات التركيب لمكونات المشروع:

أ. يجب على العارض أن يقوم بتركيب مكونات المشروع في مبنى الإدارة على النحو التالي:

1. المكونات المركزية في مركز المعطيات في الطابق 1- مثل المخدمات وأجهزة التوجيه وأجهزة الاتصال وما إلى ذلك في خزانات مناسبة يقدمها المتعهد.
2. المكونات الأخرى مثل محطات العمل وشاشات المراقبة وغيرها ستكون موجودة داخل غرفة التحكم والإدارة في المركز في الطابق 2.
3. تقديم جميع التجهيزات والبرمجيات اللازمة لأداء عملية الربط والتوصيل المناسبة بين مكونات المشروع عبر شبكة مادية منفصلة وآمنة.

ب. يجب على العارض إعداد غرفة التحكم والإدارة على النحو التالي:



1. تأمين مدخل الغرفة بالأدوات الأمنية المناسبة.
2. تأمين التحكم في الوصول.
3. تأمين نظام مراقبة - للمدخل وداخل الغرفة - بكاميرات عالية الجودة تركيب بطريقة آمنة لحمايتها من العبث ومسجل فيديو رقمي وبسعة تخزينية تكفي لتسجيل /60/ يوم على الأقل.
- ج. يجب على المعارض تصميم الشبكة والبنية التحتية الأمنية المرتبطة بها بحيث تكون معزولة فيزيائياً وأمنة.
- د. يجب على المعارض توصيف جميع مكونات المشروع (من عتاد صلب وبرمجي ضمن كل قسم ضمن المركز والسياسات والإجرائيات... إلخ) والشبكة المقترحة بشكل صريح وواضح.
9. الشروط والمواصفات الفنية:

- أ. تُعتبر الشروط والمواصفات الفنية الواردة أدناه الحد الأدنى المقبول فنياً. ويمكن للمعارض تقديم مواصفات فنية أعلى وأفضل مع بيان المميزات الفنية التي توفرها هذه المواصفات المقترحة، وتؤخذ هذه المميزات بعين الاعتبار - إن كانت مفيدة - أثناء تقييم العرض الفني.
- ب. يجب أن يكون الحل المقترح من قبل المعارض يحقق الأداء والتوافرية العالية والعمل بشكل آمن لكل مكونات المشروع.
- ج. يجب على المعارض تقديم جميع التجهيزات والبرمجيات التي تؤدي مهام ووظائف مكونات المشروع التالية وتركيبها وتنصيبها وإعدادها وتوصيلها شبكياً بالشكل الأمثل.

#### 1. مركز العمليات الأمنية

- أ. يجب على المعارض إنشاء مركز العمليات الأمنية للمشروع القادر على القيام بالمهام التالية على الأقل:

- OSS Operational support systems.
- Threat inelligence and early warning detection system.
- Alert and notification, security incident reporting.
- SOC processes, procedures and workflows.
- Cyber incident offense management.
- Proactive monitoring, network and security and server infrastructure.

- ب. يجب على المعارض تقديم وتنصيب وإعداد ومعايرة برمجية/ برمجيات SEIM القادرة على القيام بالمهام التالية:

- Collect logs, events and machine data from any source.
- Real-time application of correlation rules.
- Real-time application of advanced analytics and machine learning.
- Long-term historical analytics and machine learning.
- Long-term event storage.

- Search and reporting on normalized data.
- Search and reporting on raw data.
- Ingestion of context data for additional correlation and analytics
- Address non-security use cases
- Indexes volume: 10GB/day minimum.

ت. تفضل التراخيص الدائمة لبرمجية SIEM على السنوية.

ث. تقديم شاشات عرض جدارية بعدد مناسب للحل الفني لمركز العمليات الأمنية المقدم لعرض البيانات والمراقبة في الزمن الفعلي بحيث تكون بحجم مماثل لحجم الشاشات الموجودة مسبقاً ومتوافقة مع الحل الفني المقدم وتركب بطريقة مماثلة ويفضل أن تكون من اللون والنوع نفسه الموجود في مخبر مركز أمن المعلومات.

## 2. وحدة تقييم الثغرات واختبار الاختراق

- أ. تقوم هذه الوحدة بتحديد وتقييم وجود ثغرات وتهديدات ونقاط ضعف أمنية معروفة في مجال تكنولوجيا المعلومات و/أو أجهزة الشبكة و/أو غيرها.
- ب. كما يشمل التقييم الأمني أيضاً الثغرات الناتجة عن الإجراءات والإعدادات مثل الإعدادات الخاطئة وضعف تصميم الشبكات وسياسات الأمن.
- ج. إجراء تحليل وتحقيق من الثغرات المشتبه بها في التجهيزات والبرمجيات من خلال الفحص الفني عن ثغرات التجهيزات والبرمجيات، واقتراح الحل المناسب.
- د. إجراء المسح الداخلي والخارجي لجميع أنواع الثغرات والتهديدات ونقاط الضعف في الشبكات والمواقع الإلكترونية وتطبيقات الويب وأنظمة التشغيل وأجهزة الأمن والتطبيقات البرمجية بما فيها تطبيقات الهواتف المحمولة وأنظمة قواعد البيانات وأجهزة الشبكة وغيرها.
- هـ. إيجاد قاعدة بيانات كاملة ومفصلة وحديثة حول جميع أنواع وأحدث الثغرات والتهديدات الأخرى.
- و. اختبار تطبيقات وأنظمة قواعد البيانات وأنظمة الشبكة المحمية، متضمناً القدرة على تخمين بيانات تسجيل الدخول لأسماء المستخدمين وكلمات المرور باستخدام الأساليب الشهيرة للقيام بذلك.
- ز. إنشاء تقارير مفصلة وكاملة حول الثغرات والتهديدات ونقاط الضعف بالإضافة إلى الحلول المقترحة لكل منها، وإتاحة إمكانية تخصيص التقارير.
- ح. جمع معلومات فنية حول الأهداف مثل إصدارات البرمجيات والمنافذ المفتوحة وإدارة الخدمات وغيرها.
- ط. محاكاة الأنواع المعروفة من الهجمات وخاصة هجمات الهندسة الاجتماعية مثل رسائل التصيد مع الروابط وإعداد الملفات تسوية للأنظمة المستهدفة.

ي. إنشاء ملفات ونصوص برمجية تنفيذية تكون آلية ومخصصة لاستغلال الثغرات المكتشفة، وحقنها في الأهداف مع إمكانية التخفي وتجاوز برامج مكافحة الفيروسات وتجهيزات الحماية وغيرها من الحلول الأمنية.

ك. دعم القدرة الكاملة على استغلال جميع أنواع الثغرات والتهديدات ونقاط الضعف، ويجب على المعارض ذكر جميع طرق الاستغلال المدعومة.

ل. يجب على المعارض تقديم الرخص التالية على الأقل، ويتم تنصيبها على حواسيب محمولة عالية الأداء، بحيث تحقق المواصفات السابقة:

- نسخة مرخصة عدد/1/ لمدة سنتين لبرنامج التقييم الأمني للشبكات والتطبيقات ونظم التشغيل.
- نسخة مرخصة عدد/1/ لمدة سنتين على البرنامج التقييم الأمني لمواقع وتطبيقات الويب.
- نسخة مرخصة عدد/1/ لمدة سنتين لأداة اختبار الاختراق Penetration Testing Tool.

### 3. وحدة التحليل

أ. يجب على هذه الوحدة إجراء تحليل لأي ملف أو كائن أو نص برمجي موجود على نظام تشغيل قد يتسبب بأعمال ضارة، مثل الفيروسات والديدان وأحصنة طروادة والأبواب الخلفية وغيرها، والتي يمكن أن تعمل على نظم التشغيل المعروفة (MAC, Linux, Windows) كذلك نظم تشغيل الهواتف الذكية Android & IOS.

ب. تحليل التطبيقات والبرامج لتحديد ما إذا كانت هذه التطبيقات لها أي نشاطات ضارة على النظام.

ج. تقديم أدوات متخصصة لهذه الأغراض، وتقوم بإنشاء تقارير مفصلة.

د. تقوم بإجراء أنواع التحليل التالية:

#### 1. Static analysis:

- Determining file type and detecting packets or protectors, strings extraction and analysis, Portable executable (PE) headers analysis.
- Import table analysis, resources analysis.
- Scanning file for embedded objects (executable, images, etc.).
- The analysis shall carry out reverse engineering the source code and understand its logic to analyze the malware functionality and the algorithms used.

#### 2. Behavioral analysis:

- Performs detecting new process creation.
- Detecting file system and registry changes, detecting rootkit artifacts.
- Analyzing in-memory strings, and monitoring system events.



- This analysis should be executed on a dedicated virtual machine and proper security precautions should be taken.
- This analysis shall determine which operating system the artifact object can be executed in.

### 3. Network analysis:

- During network analysis, the malware sample is executed in a controlled environment while all network traffic is captured.
- The unit shall check what hosts the malware was communicating with and searches for any well-known network traffic patterns.
- The unit shall identify the particular malware family, addresses of command and control (C&C) servers and specific botnet to which a malware belongs.

### 4. وحدة استعادة البيانات

أ. تتطلب هذه الوحدة أداة استرداد بيانات محمولة على كمبيوتر محمول آمن عالي الأداء مع نظام تشغيل مستقر، يجب أن تلبى الأداة المتطلبات التالية على سبيل الذكر لا الحصر:

1. Compatible with work platforms: the most famous and latest versions of Windows, Linux and Mac OS.
2. Supported most famous and latest file systems that shall include all operating systems.
3. Scan for Known File Types (raw file recovery): if the disk file system is heavily damaged or unsupported, such known file types can be custom-defined.
4. Recognition and parsing of Basic (MBR), GPT, and BSD (UNIX) partitions layout schema and the Apple partition map. Support for Dynamic volumes (Windows 2000-2016/8.1/10) over MBR and GPT.
5. Support damaged RAID recovery: So for the following standard levels RAID 0, 1, 4, 5, 6. nested at least.
6. Automatic RAID parameter recognition for RAID 5 & 6 levels at least.

7. Creates image file for an entire Hard Disk, Partition or its part. Then the image files can be processed like regular disks.
8. Data recovery on damaged or deleted partitions, encrypted files, alternative data streams (NTFS, NTFS5), from NTFS with data deduplication.
9. Recover all types of data including audio and sound files Documents, e-mail messages, archive files, compressed files and folders. Can run or view them before they are restored and edit the files in hexadecimal editor before the restore process. No limit to the size of the file, the number of files that can be restored, or the size of the storage that can be scanned and the contents are retrieved.
10. Work locally or remotely over the network: Data can be restored from storage media directly or indirectly and can store recovered data locally or in other storage devices.
11. Capable of detecting and dealing with all storage media connected to the computer and whatever (USB flash memories, hard disks, CDs, DVDs, Memory Cards, etc...) and recover data from or in part when:
  - Significantly reduced.
  - Formatted.
  - Data were deleted or lost.
  - Loss of data after a viral attack.
  - After hard disk reassignment operations (FDISK, DISKPART)
12. After the MBR has been destroyed (for operating systems).
13. Portable Version can be installed on a removable device and run from any computer.
14. Support Forensic mode: can create a forensic report that can be presented at court hearings.

15. One main installation per license; support unlimited temporary installations for customer computers or any computer owned by licensee.

5. وحدة الاستجابة للطوارئ المعلوماتية

- أ. على العارض تنفيذ هذه الوحدة بحيث تتمكن من رصد طوارئ الحاسب والإبلاغ عنها بالاستفادة من الوحدات السابقة أو عن طريق الجهات و/أو الشركات و/أو مقدمي خدمات الإنترنت و/أو الأفراد و/أو المصادر الأخرى ويوضح العارض هذه المصادر في عرضه الفني، وتحقق هذه الوحدة المهام التالية:
- ب. يجب أن تتضمن الاستجابة الإجراءات المتخذة لحل أو تخفيف تأثير أي طارئ عن طريق تحليل المعلومات وتنسيقها وتوزيعها.
- ج. يجب أن تشمل الاستجابة الفنية تحليل الأحداث الواردة، والتخطيط للاستجابة المناسبة، وتنسيق الإجراءات داخلياً وخارجياً، والتي تحتوي على أي نشاط ضار مستمر، واستراتيجيات التخفيف من الآثار، وإصلاح أو استرداد أي أنظمة متأثرة، وتنفيذ تقارير وتوصيات تحليل ما بعد الحادثة، وتنفيذ إنهاء الطوارئ.
- د. يجب على العارض تقديم المعدات أو مجموعة أدوات استجابة متخصصة والتي تعمل على حواسيب محمولة آمنة وعالية الأداء مع نظام تشغيل مستقر.

9.1 متطلبات أخرى

- أ. يجب على العارض أن يقدم حواسيب محمولة عالية الأداء عدد 5/ على الأقل من أجل تلبية متطلبات المشروع وعمله بالشكل الأمثل.
- ب. تقوم الإدارة بتقديم جميع محطات العمل الحاسوبية لتنصيب البرمجيات التي يتطلب عملها تنصيبها على هذه المعدات ويحدد العارض العدد المطلوب والسبب في عرضه الفني.
- ج. يجب على العارض تقديم وتنصيب وإعداد أداة لتحليل ملفات السجل (log file analyzing tool)، يمكنها استعراض وتحليل كافة صيغ ملفات التسجيل وبعدد وحجم غير محدودين لهذه الملفات ومهما كان عدد أسطر ملف السجل، ويجب على هذه الأداة أداء وظائف التحليل الكاملة وتوليد تقارير مناسبة.
- د. يجب على العارض حجز وتقديم نطاق عالمي (.com, .net, ..) و/أو حساب بريد إلكتروني خارجي (حسب الحاجة) لمدة 5 سنوات على الأقل يخصصان لأغراض تراخيص وحسابات البرمجيات والمكونات الخاصة بالمشروع وتسلم هذه الحسابات كافة للإدارة.
- هـ. يجب على العارض تصميم وتشغيل موقع إلكتروني يعمل ضمن مركز المعطيات الوطني في الهيئة، ويحجز له نطاق علوي سوري تختاره وتقدمه الهيئة.

لموافقة



1. مخصص لمجال عمل المركز بحيث يحقق التواصل الفعال مع الزائرين وتقديم خدمات المركز والنشر والتوعية الأمنية ويدعم إبلاغ المركز بالحوادث الأمنية وفق نماذج مخصصة لهذه الغاية وبعيد عن التعقيد وسهل الإدارة والتنقل بين الصفحات
2. يجب أن يبنى الموقع الإلكتروني ضمن بيئة تفاعلية وديناميكية قابلة للتطوير دون الحاجة إلى تراخيص جديدة.
3. أن يكون تصميم الموقع الإلكتروني متوافقاً مع أحدث معايير تقنيات برمجة مواقع الويب المعيارية.
4. أن يبنى الموقع الإلكتروني بمنطق نظام إدارة محتوى ( Content Management System ) التي تتيح الإمكانية الكاملة لإدارة كافة محتويات الموقع الإلكتروني والتعامل معه وتحديثه من قبل موظفي الإدارة ودون العودة إلى المتعهد عن طريق متصفح الويب.
5. متطلبات الإدارة والسماحيات: إمكانية إدارة الموقع الإلكتروني، تنظيم المستخدمين، تنظيم أدوار المستخدمين، منح صلاحيات للأدوار وصلاحيات فردية للمستخدمين، تشمل بشكل أساسي إدارة صفحات الموقع، تعريف المساحات، التحكم بالنشر والتخزين الاحتياطي و الاستعادة، الأمن والحماية، إحصائيات الموقع الإلكتروني... إلخ.
6. على المتعهد تسليم الكود المصدري للموقع للإدارة.
7. أن يكون الموقع متوافقاً ومتناسقاً من حيث الشكل مع مختلف شاشات الحاسب والموبايل والتابلت (Responsive).
8. إمكانية إضافة عدد لا نهائي من الصفحات وتوزيعها في أقسام لتسهيل عملية التصفح والعرض والإدارة، وعلى الصفحات مع إمكانية تعديل وتنسيق محتويات الصفحة بواسطة محرر نصوص يشبه برنامج الورد word.
9. إمكانية مشاركة الصفحة على مواقع التواصل الاجتماعي مثل ( Facebook, Twitter, Whatsapp, Linkedin, Instagram, Google+...etc ).
10. إمكانية إضافة واجهة اشتراك بالقائمة البريدية في أي صفحة من صفحات الموقع .Multi Layers Architecture
11. الأمان والحماية: لتحقيق أعلى درجات الأمن للموقع الإلكتروني يجب أن تطبق أحدث إجراءات الأمن على برمجة الموقع الإلكتروني، بالإضافة لتحقيق ما يلي:
  - حماية الصفحات الداخلية للموقع الإلكتروني (مثل لوحة التحكم).
  - قدرة الموقع الإلكتروني على التصدي لأي محاولة لتكرار الطلب http requests وحجب عنوان IP المسبب للطلبات المتكررة.
  - لا يمكن لزوار الموقع الإلكتروني رفع أي ملف تنفيذي أو مكتبة ارتباط حيوي DLL.
  - خلو الموقع من الثغرات الأمنية.

- قناة اتصال مشفرة تستخدم البروتوكولات الآمنة مثل HTTPS على سبيل الذكر لا الحصر مع شهادة SSL نظامية.

و. تقديم وتنصيب وإعداد نظام بريد الكتروني مخصص للمشروع وربطه مع الموقع الإلكتروني موضوع البند السابق.  
 ز. في حال كان الحل المقدم من قبل العارض يتضمن تنصيب نظم تشغيل من نوع windows للحواسيب أو المخدمات يجب أن يلتزم العارض بتقديم وتنصيب رخص نظامية لبرامج الحماية من البرمجيات الخبيثة ذات تصنيف عالمي جيد وبالعدد اللازم.

ح. تقديم وتنصيب وإعداد رخصة نظامية لأداة مسح الشبكات ورسم الخرائط الشبكية (network mapper) تنصب على حاسب محمول من موجودات المركز، يجب أن توفر هذه الأداة جميع المواصفات التالية:

- Automate device discovery and mapping.
- Build multiple maps from a single scan.
- Export network diagram.
- Auto-detect changes to network topology.
- Perform multi-level network discovery.

## 10. اختبار المشروع

كجزء من تنفيذ المشروع، يجب على المتعهد إجراء اختبارات مختلفة وفق خطة الاختبار المقدمة من قبله لإثبات امتثال الحل المقدم لمتطلبات عمل المشروع.

## 11. التشغيل

- أ. يجب على العارض أن يقدم خطة مفصلة لكافة عمليات التشغيل ضمن عرضه الفني.
- ب. يجب على المتعهد أن يوفر الموارد البشرية الضرورية لمساعدة الإدارة لإدارة وتشغيل المشروع لفترة ثلاث أشهر بعد صدور محضر الاستلام الأولي للمرحلة الأولى، وتعمل تحت إشراف الإدارة.
- ج. يقدم العارض السير الذاتية والخبرات العملية للموارد البشرية المقدمة من قبله موضوع البند السابق في عرضه الفني.
- د. يجب أن تتضمن قائمة المهام المطلوب أداؤها من قبل المتعهد المهام التالية (على سبيل الذكر لا الحصر):

- إدارة وتشغيل المشروع.
- نقل الخبرة وتدريب العاملين في المركز ورفع سوية خبراتهم وأدائهم، وتأدية المهام بحرفية عالية وبشكل يومي.
- تحديث إجراءات الأمن المتعلقة بالمشروع والسياسات والوثائق الأخرى المتعلقة بكافة معايير وإجراءات التشغيل بموافقة الإدارة.

لمستأجر

- يجب على المتعهد تقديم عدة سيناريوهات (DRILLS) لمحاكاة عدد من الحالات الطارئة المفترضة والاستجابة لها وتنفيذها بجميع مراحلها وإجراءاتها بما يسهم في نقل الخبرة للعاملين لدى الإدارة.
- إعلام الإدارة بالأعمال الجارية وتقديم تقارير شهرية بالمهام المنجزة.
- هـ. يجب على العارض أن يدرج في عرضه قائمة مفصلة بالأدوار المقترحة للموارد البشرية المقدمة كجزء من عرضه المقدم حتى ولو لم يتم ذكرها في دفتر الشروط الفني. يجوز للإدارة أن تقرر أن بعض الأدوار يمكن أن يؤديها نفس الشخص.
- و. يجب أن يضمن العارض توفير بديل مؤقت مساو أو أعلى بالكفاءات لأي موظف مقدم سابقاً غادر بشكل (مؤقت أو دائم) المركز. يجب أيضاً ضمان استبدال الموظفين خلال أي مغادرة طارئة لأي من الأدوار المقترحة خلال فترة زمنية لا تتجاوز الأسبوع.
- ز. يحق للإدارة تغيير أي من العاملين المقدمين من قبل المتعهد في حال أنه لا يستطيع القيام بالمهام المطلوبة منه بالمستوى المطلوب، وفي مثل هذه الحالات يجب على العارض تقديم بديل خلال مدة لا تزيد عن 7 أيام.
- ح. يجب على العارض تقديم اتفاقية مستوى الخدمات (المتوافقة مع أفضل الممارسات والمعايير الشهيرة) لجميع التجهيزات والتطبيقات والبرمجيات المقدمة، مثل إجراءات تشغيل المشروع، إجراءات النسخ الاحتياطي وإجراءات تحديث النظام، وإجراءات الأمان، الاسترداد عند الفشل، إجراءات تحديث المحتوى، وإجراءات الترقية. يجب تقديم كل هذه الإجراءات والوثائق للمراجعة والموافقة عليها من قبل الإدارة قبل اعتمادها.
- ط. يجب على العارض أن يقترح ويقدم وينفذ الإجراءات والعمليات المناسبة لضمان أن مكونات المشروع بأكملها داخل مركز المعطيات متاحة في جميع الأوقات. يجب أن يتبع كل التحديثات إجراءات واضحة تسمح بتنفيذ المهام من قبل الموظف بأدوار واضحة ومحددة.

## 12. التدريب

- أ. يجب على العارض أن يقدم خطة التدريب ومواضيع الدورات في عرضه الفني، بحيث تغطي عدة مستويات من المبتدئ إلى الاحترافي وعدد المتدربين لكل مستوى ويراعى في خطة التدريب تسلسل تقديم الدورات بحيث تبدأ من تصنيف مبتدئ ثم متوسط ثم متقدم، كما يحدد عدد الساعات التدريبية لكل دورة.
- ب. يجب على المتعهد توفير التدريب الداخلي (ضمن معاهد تدريب ذات سمعة جيدة) للعاملين عدد 10/ على الدورات التالية:

1. CEH: Certified Ethical Hacker.
2. CCNA Security
3. Essential of Programming languages (like ruby & python).



ج. ففب على العارض فوففر الفرفب الفارفف للعاملفن عءء /4/ فسمفهم الفءارة على الفورات الفالفة؁ وفمكن للعارض أن فءءم فورات ففرفففة فضاففة فراها مناسفة لعمل فشففل المشروع؁ كما فمكنه اسفبءال فورة ففرفففة بأخرى شرط أن فكون بنفس المفال وففطف نفس المضمون والماءة العلمفة للفورة المطلوبة على أن فففن ذلك فف عرفضه الفنف:

1. Malware analysis.
2. Advanced Penetration Testing.
3. Advanced Windows Exploitation.
4. Advanced Web attacks and exploitation.
5. GCIH Certified Incident handler.
6. Data Recovery Training.
7. CISSP Certified Information Systems Security Professional.
8. CISM Certified Information Security Manager.

ء. ففب على العارض أن فءءم المواء الففرفففة لففمف الفورات المءلفة والفارفففة وشهاداف الفضور بالفغة الإنفلفزفة.

ه. على العارض فءءفم فكلفة كل فورة ففرفففة لكل شففص بما فف ذلك فكلفة الإقامة والسفر (للفرفب الفارفف) فف عرفضه المالي؁ كذلك فففرع عءء المفررفن المناسف لكل فورة ففرفففة أو لكل مسفوى؁ فففف فففف فففففف الأمفل للمشروع.

و. ففب أن فحصل فطة الفرفب على موافقة الفءارة.

### 13. الفوائق

أ. ففب أن فوفق المفعه فمفف عملفاف الفصفم والفنفذ والفشفل المسفءءمة فف بفئة المشروع بنسف بالفغة العربفة والإنفلفزفة.

ب. ففب أن فشمف الفوائق المقءمة من قبل المفعه على سبفل المفال لا الفصر ففففاف لمكوناف النظام وأءلة الفءارة/المسفءم مع فوائق الفركفب والففففة والفصافم الفففففلة النفاففة للمشروع وكذلك وصف مفصل لكافة عملفاف الفشفل. وأفضاً ففب أن فشمف على سبفل المفال لا الفصر فوففر السفافاف الأمففة والفشفللفة؁ والقواعد؁ والإفراءاف الضرورفة لفشفل المشروع؁ مع فءفء المعارف العالمفة الفف اسفءء علفها المفعه فف فطوفر السفافاف الفشفللفة وكافة الفوائق الفف فسفنء إلى معارف عالمفة.

ج. فلزم العارض بالسفافاة الوطنفة لأمن المعلوماف ولوائفها الفففففمة كمعار فف فطوفر كافة السفافاف الأمففة على كافة المسفوافاف والضرورفة لفشفل المشروع.

ء. ففب على العارض أن فءءم فوائق فقففة وكاملة ومءءة للءلول المقءمة. ففب أن فكون الفوائق فالفة من أف عفف أو عءم الفقة أو النقص الذف فء فؤءف إلى فءهور أءاء النظام وعءم اسفءام فءراف النظام وفقلفل موثوقفة الأنظمة وصفافها.

هـ. يجب على المعارض أن يقدم أي وثائق صيانة ضرورية. يجب أن تتضمن هذه الوثائق جميع الأدلة اللازمة لجميع التجهيزات والبرمجيات وتطبيقات المشروع متضمناً الوقاية والصيانة والتصحيح.  
و. يجب كتابة مجموعة من الأدلة لكل مستوى الصيانة. وسوف تشمل هذه: الأدلة:

1. Information necessary for conducting fault analysis and isolation.
2. Repair instructions.
3. Spare part catalogues that identify parts required for preventive and corrective maintenance including OEM part numbers as well as part numbers assigned by value added reseller or assembler.
4. Instructions and procedures for project performance and tuning.
5. Test equipment requirements and references to other manuals for their safe operation and use.
6. Safety warnings and cautions necessary for personal and resource protection

#### المصطلحات

العربي	الإنكليزي
التوافرية	Availability
شبكة روبوت	Bot-net
	DELL
عملية محاكاة هجمات سببرانية حقيقية والتصدي لها بغرض التدريب	DRILLS
برتوكول نقل النصوص	HTTP
تصميم عالي المستوى	High Level Design
برتوكول الإنترنت	IP
تصميم منخفض المستوى	Low Level Design
مفتوحة المصدر	Open Source
نظام الدعم التشغيلي	OSS
الأداء	Performance
مصفوفة مكررة من أقراص مستقلة	RAID
التكرارية	Redundancy

Portable Executable (PE)	قابل للتنفيذ محمول
Root-Kit	الجزور الخفية
NDA	وثيقة عدم إفشاء
SEIM	أمن المعلومات وإدارة الأحداث
Single Point of Failure	نقاط الفشل المفردة
SOC	مركز العمليات الأمني
SSL	طبقة المقبس الآمن

م. لبنى الجبواي



م. إياد العبود المحيسن



ماجد إسماعيل



باسل صالح



رئيس اللجنة

م. علي علي



د.م. مازن المحمد



م. سليمان سليمان



م. فادي إبراهيم

