الجمهورية العربية السورية

وزارة الاتصالات والتقانة

الهيئة الوطنية لخدمات الشبكة

الهيئة الوطنية لخدمات الشبكة
National Agency For Network Services

عدد الصفحات: 21

دفتر الشروط الخاصة الفنية

لتوريد وتركيب وإعداد واختبار وتشغيل

مشروع الاستجابة للطوارئ المعلوماتية بمركز أمن المعلومات

في الهيئة الوطنية لخدمات الشبكة

التصنيف: عادي

2020

1. 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. 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 تقديمه حتماً.
- 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، ويوفر 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. تطوير بنية لتنسيق الاستجابة للحوادث المعلوماتية الطارئة على المستوى الوطني وتحديد زمن الاستجابة لها.

هـ. تطوير القدرة على دعم الإبلاغ عن الحوادث عبر مجموعة واسعة من الطرق والأساليب بما يضمن السرعة والدقة.

و. إدارة الحوادث ونقاط الضعف والثغرات والتهديدات ودراسة وتحليل كل ذلك وتوثيق النتائج.

ز. إجراء الدراسات والأبحاث وتطوير الخبرات المعرفية في مجال الأمن المعلوماتي وذلك على المستوى الوطني.

ح. دعم ومساعدة الجهات داخل البلد على تطوير قدراتها الخاصة في إدارة الحوادث المعلوماتية.

ط. نشر التوعية وثقافة أمن المعلومات باستخدام كافة الوسائط المتاحة، كتوفير توجيهات عامة لتأمين الشبكات والتجهيزات والموارد الأخرى.

ي. تطوير مواد التدريب والتوعية بأنواعها وبكافة مستويات المستخدمين المستهدَفين من المستخدم الفرد العادي إلى مدراء ومشرفي 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: 3937047 11 963+
3. الفاكس: 3937079 11 963+
4. العنوان البريدي: دمشق – الصبورة – 60.

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

4. ملخص الأعمال العقدية

أ. إنشاء مركز العمليات الأمنية (SOC) القادر على استيعاب مراقبة واكتشاف وتحليل الحوادث المعلوماتية في الزمن الفعلي وإدارة آليات الاستجابة والمعالجة في كل من:

1. مركز المعطيات الوطني.
2. الشبكة الحكومية الآمنة.

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 والمنظومات المكونة للمشروع موضوع التعهد بما فيها اتصالات الشبكة اللازمة للمشروع.

د. توريد وتسليم وتركيب جميع البرمجيات وتطبيقات المنظومة مع التراخيص اللازمة ذات الصلة.

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 ضمن الحل الفني 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. تقديم 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.

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 البرمجيّات أو التّجهيزات أو منظومات الاتّصال خلال مدّة 3 أشهر من بدء التّشغيل.

ب. تلبية متطلبات أمن المعلومات بحيث يعمل المشروع بشكل آمن (خلو المشروع من نقاط الضعف والثغرات الأمنية).

ج. يجب أن يكون المشروع مصمماً ومنفذاً ومخصصاً بسهولة وبعيد عن التعقيد.

د. خلوّ المشروع من نقاط الفشل المفردة.

هـ. يجب ألا تقل التوافرية بالنسبة للمشروع أو أحد مكوناته عن 99.999٪.

و. تقوم الإدارة بتقييم نجاح المشروع في ظروف التشغيل خلال المرحلة الثانية من تنفيذ المشروع، ويجب على المتعهد تقديم واستدراك كل ما يلزم لتحقيق وقياس مؤشرات أسس نجاح المشروع وفق متطلبات الإدارة.

6. 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 متكاملاً، أي مشروع 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 وملاءتها الفنية.

هـ. يجب أن تكون التجهيزات والبرمجيات المقدمة من إنتاج شركات متخصصة وذات سمعة جيدة في هذا المجال، وأن تكون جديدة وغير مجددة، ومن أحدث الطرازات المنتجة بتاريخ تقديم العرض الفني.

و. يجب أن يكون العرض المقدم للمشروع من قبل العارض مرناً وقابلاً للتوسع عند الحاجة.

ز. يجب أن يكون الحل المقدم من قبل العارض معيارياً وقابلاً للتطوير ويمكن ترقيته بمرونة، كما يجب أن يقدم العارض وصفاً مفصلاً حول هذه الميزات والحدود القصوى لعمل المشروع وفق الحل المقدم من قبله جنباً إلى جنب مع المتطلبات التفصيلية

لزيادة السعة إلى الحد الأقصى الممكن دون الحاجة إلى تغيير المكونات الأساسية للمشروع أو استبدال الأجهزة أو البرمجيات الأساسية.

ح. تم إعداد هذا الدفتر بعناية وذلك بعدم ترك أي غموض في الأعمال المطلوبة، وفي حال فشل العارض في فهمه أو الحاجة 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، ويقوم العارض بنفسه بقياس جميع المؤشرات وجمع المعلومات التي يحتاجها لتقديم عرضه الفني بالتنسيق مع الإدارة.

ي. يجب على العارض مراعاة موجودات مركز أمن المعلومات والمذكورة لاحقاً ودمجها في الحل المقدم من قبله، وترقيتها –في حال وجود حاجة لذلك– بحيث يتم استثمارها في المشروع بالشكل الأمثل.

ك. يجب على العارض تقديم إجابة كاملة ومفصلة ودقيقة عن هذا الدفتر بنداً بنداً في عرضه الفني، والذي يشمل:

- 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 تشمل العلامة التجارية والطراز والنسخة، وبلد التصنيع وشركة التصنيع وعام التصنيع/الإنتاج.

م. تُفضّل التراخيص الدائمة على التراخيص السنوية، وستحدد الإدارة الاختيار المناسب، ويجب على العارض أن يقدم بعرضه قائمة مفصلة بجميع تراخيص التجهيزات والبرمجيات.

ن. يجب على العارض أن يقدم عرضاً لتجديد التراخيص للبرمجيات والتجهيزات التي يتطلب عملها رخصاً نظامية وذلك للأعوام الخمسة القادمة وبأسعار يتفق عليها في حينه، 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 أو متطلبات ذات قيمة مضافة غير مذكورة في دفتر الشروط هذا وفوائد هذه الميزات وستؤخذ الميزات الإضافية –إن كانت مفيدة– بعين الاعتبار عند إجراء التقييم الفني.

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

ف. يجب أن تدعم البرمجيات والتجهيزات الشبكية المقدمة بروتوكول العنونة بالإصدار السادس IPV6 بالإضافة إلى العنونة بالإصدار 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).
3. مخططات سير العمليات في جميع مكونات المشروع.

4. الهيكل التنظيمي (الإداري) المتوافق مع الحل الفني المقدم ويشمل الحد الأدنى من الموارد البشرية المطلوبة لتشغيل المشروع مع مهامهم ومسمياتهم الوظيفية.

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

ر. يجب على العارض توصيف جميع مكونات المشروع (من عتاد صلب وبرمجي ضمن كل قسم ضمن المركز والسياسات والإجرائيات ...إلخ) والشبكة المقترحة بشكل صريح وواضح.

ش. يجب على المتعهد الالتزام بتقديم الدعم الفني خلال فترة الضمان المجاني (سنتين ميلاديتين) وبزمن استجابة لا يتجاوز ثلاث ساعات من إعلامه عن طريق الهاتف أو الفاكس أو البريد الإلكتروني أو عبر كتاب رسمي، كما يُطلب 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.

ت. 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.

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

خ. يجب أن يلتزم العارض بالسياسة الوطنية لأمن المعلومات ولوائحها التنظيمية كمعيار في تطوير كافة السياسات الأمنية على كافة المستويات والضرورية لعمل المشروع، في حال وجود متطلبات خاصة بالسياسات الأمنية لا توفرها السياسة الوطنية لأمن المعلومات يتم الاعتماد على أفضل المعايير والممارسات العالمية ذات الصلة.

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

ض. يجب على العارض تقديم تعهد خطي بتحقيق أسس نجاح المشروع كاملةً والواردة في الفقرة /5/ من هذه الوثيقة.

غ. يلتزم المتعهد بتشغيل المشروع لفترة زمنية مماثلة للمرحلة الثانية من تنفيذ المشروع قابلة للتجديد أو التمديد بعد صدور محضر الاستلام الأولي لكامل المشروع، وبنفس الشروط والمواصفات والمهام المطلوبة من المتعهد في المرحلة الثانية من تنفيذ المشروع وبنفس الأسعار العقدية، في حال طلبت الإدارة التجديد أو التمديد.

7. شروط رفض العرض الفني:

يعتبر العرض مرفوضاً فنياً في الحالات التالية:

1. عدم اطلاع العارض على موقع العمل والأعمال الواجب إنجازها ومواصفات التجهيزات والبرمجيات الموجودة مسبقاً في المركز أو موقع العمل قبل تقديم العروض الفنية والمالية وتقديم تصريح يثبت ذلك.
2. وجود تحفظ على أي من بنود دفاتر الشروط الفنية أو الحقوقية أو المالية.
3. تقديم العارض لجزء من الكميات المطلوبة دون تقديم الكميات الأخرى.
4. تقديم العارض لتجهيزات مجددة أو غير جديدة أو مجمعة محلياً.
5. تقديم تجهيزات أو برمجيات برخص مقرصنة.

6. توقف عمل المشروع بانتهاء صلاحية التراخيص.
7. وجود نقطة فشل مفردة تؤدي إلى توقف عمل المشروع.

8. تنفيذ المشروع:

ينفذ المشروع على مرحلتين:

- **المرحلة الأولى**: ومدتها /150/ يوماً، وتتضمن تنفيذ كافة أعمال التوريد والتركيب والتنصيب والإعداد والاختبار والتدريب المطلوب خلالها (وفق خطة التدريب المقدمة من العارض) وإعداد وتقديم جميع الوثائق المطلوبة في هذا الدفتر أينما وردت، وتبدأ من اليوم التالي لتاريخ تبليغ المتعهد أمر المباشرة.
- **المرحلة الثانية**: وهي مرحلة التشغيل ومدتها /90/ يوماً، وتتضمن تنفيذ كافة أعمال التشغيل والتدريب المطلوب خلالها (وفق خطة التدريب المقدمة من العارض)، وتبدأ اعتباراً من اليوم التالي لتاريخ إعلام المتعهد بمصادقة الإدارة على محضر الاستلام المؤقت للمرحلة الأولى.

9. 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 وآمنة. 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".

9.1 المكونات الحالية للمخبر الوطني لأمن المعلومات

أ. إن الغاية من هذا البند تعريف العارض بمكونات المخبر، وفي حال حاجة العارض لمعلومات إضافية يتوجب عليه الحصول عليها من موقع العمل، بحيث يجب على العارض دمجها واستثمارها في الحل الفني المقدم من قبله وهي:

ب.

برمجيات وتطبيقات	العدد	الوظيفة
Tenable Nessus 7 Professional	1	برنامج مسح الشبكات والنظم

Acunetix 9.5 Web Vulnerability Scanner	3	برنامج مسح تطبيقات الويب
KALI Advanced Penetration Testing OS	2	اختبار الاختراق / مسح – مفتوح المصدر
VPN Subscription	1	500 Gb: تم استهلاك معظم الحزمة
CAIN+SIFT (Data recovery +Forensic)	1	تحليل جنائي رقمي، استعادة البيانات – مفتوح المصدر
تجهيزات	**العدد**	**معلومات إضافية**
مخدم مركزي	4	أنظمة تشغيل windows pro 2008 عدد 2
محطات عمل وحواسب مكتبية	4	مع أنظمة تشغيل Windows 10 مرخصة
حواسب محمولة	5	3 مع أنظمة تشغيل مرخصة 2 بدون أنظمة تشغيل
شاشات مراقبة جدارية	2	-
وحدة حماية مركزية	1	UTM
KVM	1	-
موجه	1	Gateway
خط اتصال إنترنت	1	Fiber 20 Mbps
خط اتصال إنترنت	1	ADSL 2 Mbps
شبكة داخلية كاملة	1	مستقلة فيزيائياً عن شبكة الإدارة
وحدات عدم انقطاع التيار الكهربائي	2	10KVA, 5KVA
مبدلة شبكية L3	2	Huawei

ج.

المخدم	المعالج	الرام	الهارد	كرت الشبكة ايثرنت	كرت الشبكة Fiber
Lenovox3850	Intel xeon 4*14	128 G	2*600	4*1G	يوجد كرت فايبر
Lenovox3850	Intel xeon 4*14	128 G	2*600	4*1G	يوجد كرت فايبر

Lenovox3850	Intel xeon 4*14	96 G	2*600	4*1G	يوجد كرت فايبر

10. 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 غرف المركز في الطابق 2 ويقدم العارض رؤيته حول توزيع مكونات المشروع على غرف المركز مع تقديم التصاميم اللازمة لذلك.
3. تقديم جميع التجهيزات والبرمجيات اللازمة لأداء عملية الربط والتوصيل المناسبة بين مكونات المشروع عبر شبكة مادية منفصلة وآمنة.

ب. يجب على العارض تصميم الشبكة والبنية التحتية الأمنية المرتبطة بها للمشروع ولجميع مكوناته بحيث تكون معزولة فيزيائياً وآمنة.

11. المرحلة الأولى: الشروط والمواصفات الفنية

أ. تُعتبر الشروط والمواصفات الفنية الواردة أدناه الحد الأدنى المقبول فنياً. ويمكن للعارض تقديم مواصفات فنية أعلى وأفضل مع بيان الميّزات الفنية التي توفرها هذه المواصفات المقترحة، وتؤخذ هذه الميّزات بعين الاعتبار – إن كانت مفيدة – أثناء تقييم العرض الفني.

ب. يجب أن يكون الحل المقترح من قبل العارض يحقق الأداء والتوافرية العالية والعمل بشكل آمن لكل مكونات المشروع.

ج. يجب على العارض تقديم جميع التجهيزات والبرمجيات التي تؤدي مهام ووظائف المشروع التالية وتركيبها وتنصيبها وإعدادها وتوصيلها شبكياً بالشكل الأمثل، بالإضافة لتنفيذ وتقديم الأعمال الواردة تالياً:

11.1 مركز العمليات الأمنية Security Operation Center

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

- OSS Operational support systems.
- Threat inelegance 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 العارض تقديم وتنصيب وإعداد ومعايرة برمجية/ تجهيزة 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 النظامية لبرمجية SIEM (لا تقل عنة سنة) على التراخيص المفتوحة المصدر.

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 ويمكن ربطها شبكياً ومن خلال تقنية HDMIومتوافقة مع الحل الفني المقدم وتركب بطريقة فنية جيدة ويفضل أن تكون من اللون والنوع نفسه الموجود في مخبر مركز أمن المعلومات.

11.2 وحدة تقييم الثغرات واختبار الاختراق

أ. يحق للإدارة أن تقرر تنفيذ جميع أو بعض أعمال هذا البند، ويجب على العارض الالتزام بتقديم جميع الأعمال المطلوبة في هذه الوحدة في عرضيه الفني والمالي ووفق الشروط والمواصفات المطلوبة، بحيث تختار الإدارة ما يجب على المتعهد تنفيذه من أعمال هذه الوحدة.

ب. تقوم هذه الوحدة باكتشاف وتقييم الثغرات والتهديدات ونقاط الضعف الأمنية في مجال نظم تكنولوجيا المعلومات و/أو أجهزة الشبكة و/أو غيرها لزوم تقديم خدمات المسح والتقييم الأمني واختبار الاختراق وعلى العارض تقديم الأدوات والبرمجيات التي تحقق متطلبات هذه الوحدة.

ج. كما يشمل التقييم الأمني أيضاً الثغرات الناتجة عن الإجراءات والإعدادات مثل الإعدادات الخاطئة وضعف تصميم الشبكات وسياسات الأمن.

د. إجراء تحليل وتحقق من الثغرات المشتبه بها في التجهيزات والبرمجيات من خلال الفحص الفني عن ثغرات التجهيزات والبرمجيات، واقتراح الحل المناسب.

هـ. إجراء المسح الأمني الداخلي والخارجي (عن بعد) لجميع أنواع الثغرات والتهديدات ونقاط الضعف في الشبكات والمواقع الإلكترونية وتطبيقات الويب وأنظمة التشغيل والتجهيزات الشبكية والتطبيقات البرمجية بما فيها تطبيقات الهواتف المحمولة وأنظمة قواعد البيانات وغيرها.

و. إيجاد قاعدة بيانات كاملة ومفصلة وحديثة حول جميع أنواع وأحدث الثغرات والتهديدات الأخرى.

ز. اختبار اختراق التطبيقات ونظم التشغيل وأنظمة قواعد البيانات وأنظمة الشبكة المحمية، متضمنةً القدرة على تخمين بيانات تسجيل الدخول لأسماء المستخدمين وكلمات المرور باستخدام الأساليب الشهيرة للقيام بذلك.

ح. تتمتع البرمجيات المخصصة للمسح الأمني بميزات إنشاء تقارير مفصلة وكاملة حول الثغرات والتهديدات ونقاط الضعف بالإضافة إلى الحلول المقترحة لكل منها، وإتاحة إمكانية تخصيص التقارير.

ط. جمع معلومات فنية حول الأهداف مثل إصدارات البرمجيات والمنافذ المفتوحة وإدارة الخدمات وغيرها.

ي. إنشاء واحتواء ملفات ونصوص برمجية تنفيذية (payloads) تكون آلية ومخصصة لاستغلال الثغرات المكتشفة، أو حقنها في الأهداف المختبرة مع إمكانية التخفي ومحاكاة الهجمات الإلكترونية وتجاوز برامج مكافحة الفيروسات وتجهيزات الحماية وغيرها من الحلول الأمنية (ميزة خاصة بأداة اختبار الاختراق).

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

ل. يجب على العارض تقديم الرخص التالية على الأقل من ضمن الأدوات والبرمجيات المخصصة لهذه الوحدة، ويتم تنصيبها على حواسب محمولة عالية الأداء، بحيث يحقق المتطلبات السابقة:

- نسخة مرخصة عدد/1/ لمدة سنتين لبرنامج التقييم الأمني للشبكات والتطبيقات ونظم التشغيل.
- نسخة مرخصة عدد/1/ لمدة سنتين على الأقل للبرنامج المخصص للتقييم الأمني لمواقع وتطبيقات الويب.
- نسخة مرخّصة عدد /1/ لمدة سنتين على الأقل للبرنامج المخصص للتقييم الأمني لتطبيقات الأجهزة والهواتف المحمولة.
- نسخة مرخصة عدد/1/ لمدة سنتين لأداة اختبار الاختراق Penetration Testing Tool.

11.3 وحدة التحليل

أ. يحق للإدارة أن تقرر تنفيذ جميع أو بعض أعمال هذا البند، ويجب على العارض الالتزام بتقديم جميع الأعمال المطلوبة في هذه الوحدة في عرضيه الفني والمالي ووفق الشروط والمواصفات المطلوبة، بحيث تختار الإدارة ما يجب على المتعهد تنفيذه من أعمال هذه الوحدة.

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

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

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

هـ. 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.

11.4 وحدة استعادة البيانات

أ. يحق للإدارة أن تقرر تنفيذ جميع أو بعض أعمال هذا البند، ويجب على العارض الالتزام بتقديم جميع الأعمال المطلوبة في هذه الوحدة في عرضيه الفني والمالي ووفق الشروط والمواصفات المطلوبة، بحيث تختار الإدارة ما يجب على المتعهد تنفيذه من أعمال هذه الوحدة.

ب. تتطلب هذه الوحدة أداة استرداد بيانات محمولة على حاسب محمول آمن عالي الأداء مع نظام تشغيل مستقر، يجب أن تلبي 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, 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)
    - After the MBR has been destroyed (for operating systems).
12. Portable Version can be installed on a removable device and run from any computer.
13. Support Forensic mode: can create a forensic report that can be presented at court hearings.
14. Multi-platform licensing: Windows, Mac and Linux.

11.5 وحدة الاستجابة للطوارئ المعلوماتية

أ. يجب 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 التي يوفرها المشروع :تحليل الأحداث الواردة التي تحتوي على أي نشاط ضار ، والتخطيط للاستجابة المناسبة، وتنسيق الإجراءات داخلياً وخارجياً مع مركز العمليات الأمنية، وآليات 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 والتجهيزات والبرمجيات اللازمة لتحقيق مهام هذه الوحدة في الرصد والإبلاغ، كذلك الاستجابة لطوارئ الحاسب سواء من موقع المركز أو في مكان حدوث الحالة الطارئة (على سبيل الذكر لا الحصر مجموعة أدوات استجابة متخصصة لفريق الاستجابة والتي تعمل على حواسب محمولة عالية الأداء مع نظم تشغيل مستقرة ومعدات مخصصة لتحقيق متطلبات ومهام هذه الوحدة).

11.6. متطلبات أخرى

أ. يحق للإدارة أن تقرر تنفيذ جميع أو بعض أعمال هذا البند، ويجب على العارض الالتزام بتقديم جميع الأعمال المطلوبة في هذه الوحدة في عرضيه الفني والمالي ووفق الشروط والمواصفات المطلوبة، بحيث تختار الإدارة ما يجب على المتعهد تنفيذه من أعمال هذه الوحدة.

ب. يجب على العارض أن يقدم حواسب محمولة عالية الأداء عدد/5/ من أجل تلبية متطلبات المشروع وعمله بالشكل الأمثل (لأغراض الاستجابة للطوارئ المعلوماتية) بالمواصفات التالية على الأقل لكل منها:

1- قرص صلب نوع SSD بسعة 128GB على الأقل.
2- قرص صلب من النوع التقليدي بسعة 500GB على الأقل.
3- ذاكرة سعة 16Gb.
4- معالج Core i7.
5- بطارية غير مدمجة تدوم أكثر من 5 ساعات عمل.

ج. تقوم الإدارة بتقديم جميع محطات العمل الحاسوبية التي يتطلبها الحل الفني، ويحدد العارض العدد المطلوب والمواصفات والسبب في عرضه الفني.

د. 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.

هـ. يجب على العارض حجز وتقديم نطاق عالمي (.com, .org,..) وحساب بريد إلكتروني خارجي لمدة /5/ سنوات على الأقل يخصصان لأغراض تراخيص وحسابات البرمجيات والمكونات الخاصة بالمشروع وتسلم هذه الحسابات كافة للإدارة.

و. يجب على العارض تصميم وتشغيل موقع إلكتروني يعمل ضمن مركز المعطيات الوطني في الهيئة، ويحجز له نطاق علوي سوري تختاره وتقدمه الهيئة ويحقق مايلي:

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. على تطبيق الويب توفير نماذج تفاعلية مخصصة للإبلاغ عن الحوادث الطارئة، بالإضافة الى نماذج مخصصة لتسجيل طلبات لكافة خدمات مركز أمن المعلومات مع حل مناسب لحفظ وأرشفة هذه الطلبات ضمن قاعدة بيانات التطبيق، وعلى هذه النماذج أن تكون قابلة للتطوير والتعديل حسب الحاجة المستقبلية.
4. أن يكون تصميم الموقع الإلكتروني متوافقاً مع أحدث معايير تقنيات برمجة مواقع الويب المعيارية.
5. 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.
6. 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 والاستعادة، الأمن والحماية، إحصائيات الموقع الإلكتروني....
7. على المتعهد تسليم الرمّاز المصدري للموقع للإدارة.
8. أن يكون الموقع متوافقاً ومتناسقاً من حيث الشكل مع مختلف شاشات الحاسب والهواتف والأجهزة المحمولة (Responsive).
9. 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 شبيه ببرنامج word.
10. إمكانية مشاركة الصفحة على مواقع التواصل الاجتماعي مثل (Facebook, Twitter, Whatsapp, Linkedin, Instgram, Google+...etc).
11. إمكانية إضافة واجهة اشتراك بالقائمة البريدية في أي صفحة من صفحات الموقع
Multi Layers Architecture.
12. 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.
    - خلوّ الموقع من الثغرات الأمنية.
    - قناة اتصال مشفرة تستخدم البروتوكولات الآمنة مثل HTTPS على سبيل الذكر لا الحصر مع شهادة SSL نظامية.

ز. تقديم وتنصيب وإعداد نظام بريد الكتروني مخصص للمشروع.

ح. في حال كان الحل المقدم من قبل العارض يتضمن تنصيب نظم تشغيل من نوع windows للحواسب أو المخدمات يجب أن يلتزم العارض بتقديم وتنصيب رخص نظامية لبرامج الحماية من البرمجيات الخبيثة ذات تصنيف عالمي جيد وبالعدد اللازم.

ط. متطلبات أمن المعلومات:

1- يجب على العارض تقديم كل ما يلزم من تجهيزات وبرمجيات أمنية وإعدادها ومعايرتها بحيث يتم حماية المشروع بجميع مكوناته من الهجمات الإلكترونية الخارجية والداخلية، ويتم بيان ذلك مفصلاً وبدقة في تصميم المشروع والمخططات الشبكية التي يقدمها العارض في عرضه الفني.

2- إعداد وتقديم وثيقة تقييم المخاطرRisk Assessment ذات الصلة بأمن المعلومات لكامل المشروع، ويحدد العارض المعايير التي اعتمدها لتطوير هذه الوثيقة في عرضه الفني.

ي. يجب على العارض إعداد غرفة التحكم والإدارة للمشروع في الطابق 2 على النحو التالي:

- تأمين مدخل الغرفة بالأدوات الأمنية المناسبة (باب آمن مع وحدة تحكم تسمح بفتح القفل الإلكتروني للباب عن طريق البطاقة أو كلمة مرور أو البصمة مع حفظ سجلات دخول، وفي حال استخدام البطاقة للدخول يجب تقديم /20/ بطاقة على الأقل).
- تأمين وتركيب نظام مراقبة فديوي- للمدخل وداخل الغرفة - بكاميرات عالية الجودة تركب بطريقة آمنة لحمايتها من العبث ومسجل فيديو رقمي وبسعة تخزينية تكفي لتسجيل /60/ يوم على الأقل.

ك. 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.

11.7. اختبار المشروع

كجزء من تنفيذ المشروع، يجب على المتعهد إجراء كافة الاختبارات التشغيلية والأمنية (الأداء-التوافرية- أمن المعلومات-....) وفق خطة الاختبار المقدمة من قبله لإثبات امتثال الحل المقدم لمتطلبات عمل المشروع.

11.8. الوثائق

أ. تقدم الوثائق المطلوبة في هذه الفقرة خلال المرحلة الأولى من تنفيذ المشروع.

ب. يجب أن يوثق المتعهد جميع عمليات التصميم والتنفيذ والتشغيل المستخدمة في بيئة المشروع بنسخ باللغة العربية والإنكليزية.

ج. يجب أن تشمل الوثائق المقدمة من قبل المتعهد على سبيل المثال لا الحصر كتيبات لمكونات النظام وأدلة الإدارة/المستخدم مع وثائق التركيب والتهيئة والتصاميم التفصيلية النهائية للمشروع وكذلك وصفاً مفصلاً لكافة عمليات التشغيل. وأيضاً يجب أن تشمل على سبيل المثال لا الحصر تقديم السياسات الأمنية والتشغيلية، والقواعد، والإجراءات الضرورية لتشغيل المشروع، مع تحديد المعايير العالمية التي استند عليها المتعهد في تطوير السياسات التشغيلية وكافة الوثائق التي تستند إلى معايير عالمية.

د. يجب على العارض أن يقدم وثائق دقيقة وكاملة ومحدثة للحلول المقدمة. يجب أن تكون الوثائق خالية من أي عيب أو عدم الدقة أو النقص الذي قد يؤدي إلى تدهور أداء النظام وعدم استخدام قدرات النظام وتقليل موثوقية الأنظمة وصيانتها.

هـ. يجب على العارض 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 تقديم مجموعة من الأدلة المخصصة للصيانة .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.

12. المرحلة الثانية–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 ثلاثة أشهر بعد صدور محضر الاستلام المؤقت 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 بجميع مكوناته وبإشراف من الإدارة وبالتنسيق معها.
- تنفيذ المهام المسندة من قبل الإدارة في إطار تشغيل المشروع وبحرفية عالية.
- استمرار العمل للكوادر البشرية التي يقدمها المتعهد في المشروع خلال أوقات الدوام الرسمي وخارجه وأثناء العطل الرسمية والمناسبات والأعياد لتأدية المهام التي تتطلب وجود مناوبات بحيث يتم تقديم الخدمة بشكل مستمر 7/24.
- نقل الخبرة وتدريب العاملين في المركز على استثمار جميع التجهيزات والبرمجيات والوحدات المكونة للمشروع وبشكل عملي 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.
- يجب على المتعهد تقديم عدة سيناريوهات (DRILLS) لمحاكاة عدد من الحالات الطارئة المفترَضة 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 التي يقدمها كجزء من عرضه الفني 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 المركز بشكل مؤقت أو دائم. 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 تبين لها 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 متاحة في جميع الأوقات. يجب أن يتبع كل التحديثات إجراءات واضحة تسمح بتنفيذ المهام من قبل الموظف بأدوار واضحة ومحددة.

13. 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 والمتطلبات اللازمة (المستوى العلمي، الشهادة، ...) للمتدربين 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 من قِبل مدربين معتمدين وذلك لـ/15/ متدرب على الأقل تسميهم الإدارة، ويمكن للعارض أن يقدم دورات تدريبية إضافية يراها مناسبة لعمل وتشغيل المشروع، كما يمكنه استبدال دورة تدريبية بأخرى شرط أن تكون بنفس المجال وتغطي نفس المضمون والمادة العلمية للدورة المطلوبة على أن يبين ذلك في عرضه الفني وهذه الدورات هي:

1. Essential of Programming languages (ruby & python) /75/ hours:
   - Installation
   - Syntax
   - Declarations:
     - Data structures
     - Loops
     - Conditions
     - Exceptions
   - OOP
   - Database connections
2. Malware Analysis /30/ hours.
3. Advanced Penetration Testing /40/ hours.

4. Advanced Windows Exploitation /30/ hours.
5. Advanced Web attacks and exploitation /65/ hours.
6. CIH Certified Incident handler (60) hours

- Introduction to Incident Handling and Response
- Incident Handling and Response Process
- Forensic Readiness and First Response
- Handling and Responding to Malware Incidents
- Handling and Responding to Email Security Incidents
- Handling and Responding to Network Security Incidents
- Handling and Responding to Web Application Security Incidents
- Handling and Responding to Cloud Security Incidents
- Handling and Responding to Insider Threats

7. Data Recovery Training /20/ hours.

ج. يجب على العارض أن يقدم المواد التدريبية لجميع الدورات وشهادات الحضور باللغة الإنجليزية على الأقل.

د. على العارض تقديم تكلفة كل دورة تدريبية مع بيان الكلفة لكل متدرب وذلك في عرضه المالي، كذلك يقترح عدد المتدربين المناسب لكل دورة تدريبية أو لكل مستوى، بحيث يتحقق التشغيل الأمثل للمشروع.

هـ. يتم تقديم التدريب المطلوب في هذه الفقرة خلال مرحلتي التنفيذ للمشروع بالكامل البالغة /240/ يوماً، ويراعي العارض في ذلك (خطة التدريب) تقديم الدورات التدريبية التي تتطلب العمل على تجهيزات المشروع خلال فترة التشغيل (المرحلة الثانية).

و. يجب أن تحصل خطة التدريب على موافقة الإدارة.

14. المصطلحات

العربي	الإنكليزي
التوافرية	Availability
شبكة روبوت	Bot-net
عملية محاكاة هجمات سيبرانية 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

Performance	الأداء
RAID	مصفوفة مكررة من أقراص مستقلة
Redundancy	التكرارية
Portable Executable (PE)	قابل للتنفيذ محمول
Root-Kit	الجذور 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

لجنة الإعداد

عضواً

كمال أسعد

عضواً

عصام المشوح

عضواً

م. لبنى الجباوي

رئيس اللجنة

عضواً

ماجد اسماعيل

عضواً

م. سلمان سليمان

شوهد وصدّق

المدير العام للهيئة الوطنية لخدمات الشبكة

المهندس علي علي

دمشق / / كانون الأول 2020