






Vizualizare anunt

 PUBLICAT
  NR ANUNT: ADV1078469
  TIP ANUNT: CUMPARARI DIRECTE
  DATA CREARE: 14.05.2019 10:31
 DATA PUBLICARE: 14.05.2019 10:36

DATE IDENTIFICARE AUTORITATE CONTRACTANTA

Denumire oficiala: OFICIUL NATIONAL DE PREVENIRE SI COMBATERE A SPALARII BANILOR CIF: 11806010

Adresa: Strada General Ion Florescu, Nr. 1, Sector: 3 Tara: Romania

Tel: +40 213155207 Fax: +40 213155227 E-mail: onpcsb@onpcsb.ro Punct(e) de contact: Veronica Rata In atentia: : Veronica Rata

ANUNT

Denumire contract:

SERVICII MENTENANTA SI ASISTENTA TEHNICA

Data limita depunere oferta:

24.05.2019 10:28

Tip anunt:	Tip contract:	Cod si denumire CPV:	Valoare estimata:	Caiet de sarcini:
<u>Cumparari directe</u>	<u>Servicii</u>	<u>72611000-6 - Servicii de asistenta tehnica informatica (Rev.2)</u>	<u>20.587,00 RON</u>	<u>Caiet de sarcini mentenanta si asistenta tehnica.pdf</u>

Descriere contract:

servicii mentenanta si asistenta tehnica SROL si site ONPCSB pentru perioada 01.06.2019-31.12.2019

Conditii referitoare la contract:

cf caiet de sarcini

Conditii de participare:

cf caiet de sarcini

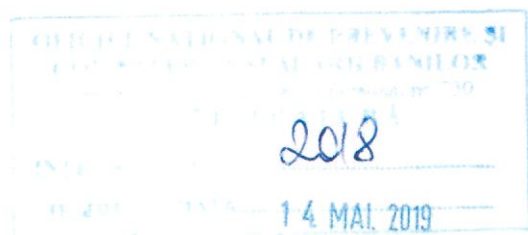
Criterii de atribuire:

PRETUL CEL MAI SCAZUT

Informatii suplimentare:

-

LISTA VERSIUNI ANUNT PUBLICITAR



De acord,

PREȘEDINTELE
Oficiului Național de Prevenire și
Combatere a Spălării Banilor

Daniel Marius Staicu



CAIET DE SARCINI

Servicii mentenanță și asistență tehnică

Caietul de sarcini definește natura serviciilor de mentenanță și asistența tehnică asigurate pentru Sistemul de raportare on-line și web-site-ul Oficiului Național de Prevenire și Combatere a Spălării Banilor, și este întocmit pornind de la resursele informatice existente. Sistemul de Raportare on-line este instalat pe două servere care funcționează în paralel și este dezvoltat în PHP, Zend Framework, Java, și are baza de date de tip MySQL. Web-site-ul este realizat în PHP + HTML + CSS.

Obiectivul este executarea de servicii de **mentenanță** pentru Sistemul de raportare on-line și web-site, pentru ca sistemele să fie complet funcționale și accesibile tuturor beneficiarilor, în permanentă, și pentru evitarea pierderii informațiilor vitale, ce ar putea aduce instituției prejudicii de imagine, de ordin financiar, etc.

I. Principalele activități care se prestează sunt:

1. Mentenanță

1.1. Servicii de mentenanță preventivă

Activitățile de mentenanță preventivă au ca scop prevenirea pe cât posibil a apariției oricărui inconvenient sau a oricărei întreruperi în funcționarea sistemelor. Activitățile de mentenanță preventivă sunt activități planificate periodic de verificare a stării de funcționare a serverelor, a aplicațiilor și a bazelor de date utilizate, precum și de realizare a copiilor de siguranță ale acestora.

1.2. Servicii de mentenanță corectivă

Activitățile de mentenanță corectivă sunt activități derulate pentru corectarea unei defecțiuni manifestate sau în curs de manifestare în cadrul sistemelor. Au rolul de a reduce cât mai mult posibil timpul de nefuncționare sau de funcționare defectuoasă a sistemelor și de a înlătura deserviciile cauzate utilizatorilor finali de anomaliile existente la nivelul sistemului. Furnizorul va investiga erorile și dificultățile care apar în funcționarea aplicației informatice pentru identificarea cauzelor care le determină, în vederea remedierii acestora.

Dacă este cazul, furnizorul va folosi copiile de siguranță pentru restaurarea bazei de date și a aplicațiilor.

Timpul de remediere, este stabilit în funcție de gravitatea incidentului, astfel:

- Incident de nivel minor – maxim 3 zile lucrătoare
- Incident de nivel major – maxim o zi lucrătoare
- Incident de nivel critic – maxim 6 ore (program de lucru)
- Incident de nivel urgent – maxim 3 ore (program de lucru)

Furnizorul va asigura menținerea instrucțiunilor de folosire a aplicațiilor (Ajutor) în conformitate cu modul curent de funcționare.

1.3. Servicii de mentenanță evolutivă

Activitățile de mentenanță evolutivă sunt activități de actualizare a aplicațiilor care constau în furnizarea de versiuni noi, în vederea satisfacerii solicitărilor de implementare a unor noi funcționalități, reguli de business noi sau modificate, precum și alte adaptări necesare datorită schimbărilor legislative, administrative sau procedurale legate de funcționarea sistemelor.

1.4. Servicii de mentenanță adaptivă

Activitățile de mentenanță adaptivă sunt activități de adaptare a software-ului aferent sistemelor care constau în actualizarea acestora, cu scopul de a le păstra funcționalitatea, disponibilitatea și de a le îmbunătăți performanțele în condițiile unor modificări intervenite în mediul în care rulează. Modificările pot fi la nivelul platformei hardware și/sau software pe care este instalată soluția.

2. Activități de instalare și configurare

În vederea îndeplinirii obiectivului prevăzut de contract, în situațiile în care activitățile de mentenanță sunt însoțite de actualizări ale sistemelor dezvoltate, vor fi desfășurate activități de instalare și configurare a soluției, ori de câte ori este necesar.

3. Activități de testare

După fiecare modificare minoră sau majoră care are loc în program se va realiza testarea unor aspecte cum ar fi: funcționarea, integritatea, performanța, securitatea aplicației, etc.

4. Servicii de suport tehnic

Serviciile de suport tehnic sunt activități de preluare și soluționare a tuturor cererilor de suport care apar în contextul derulării contractului.

5. Servicii de optimizare

Serviciile de optimizare constau în îmbunătățirea performanței aplicațiilor. Furnizorul va face recomandări pentru a îmbunătăți performanțele aplicațiilor și va stabili modificările de software și de hardware necesare, estimând costurile pe care le presupun aceste modificări.

II. Securitatea informației

Furnizorul va respecta **Politica de securitate a resurselor informatice și de comunicații** a beneficiarului.

În relația dintre Beneficiar și Furnizorul de servicii se stabilește contractual faptul că toate informațiile Beneficiarului la care furnizorul are acces sunt CONFIDENȚIALE.

Informațiile vor fi folosite numai în scopul îndeplinirii sarcinilor contractuale și nu vor fi divulgate unor terți.

În acest sens, furnizorul trebuie să dețină certificat ISO 27001.

III. Prestarea serviciilor

Autoritatea contractanta solicita disponibilitatea on-line sau on-site, după caz, în zilele lucrătoare, de luni până vineri timp de 4 ore a unui specialist care să asigure serviciile mai sus menționate și respectarea, fără excepție, a termenelor de remediere a incidentelor, pe perioada derulării contractului.

DEFINIȚII

Politica de securitate a resurselor informatice și de comunicații reprezintă totalitatea măsurilor necesare pentru asigurarea integrității, confidențialității și disponibilității informației.

- Integritatea se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate;
- Confidențialitatea se referă la protecția datelor împotriva accesului neautorizat;
- Disponibilitatea se asigură prin funcționarea continuă a tuturor componentelor sistemului.

Timp de remediere. Prin timp de remediere părțile înțeleg timpul scurs între momentul în care BENEFICIARUL notifică FURNIZORUL asupra apariției unui incident în legătură cu sistemul de raportare on-line și/sau a website-ului și momentul în care FURNIZORUL repune sistemul în stare de funcționare la parametrii conveniți.

Incident de nivel minor reprezintă o eroare care afectează o funcție sau proces, dar funcționarea întregului sistem nu este afectată sau este afectată nesemnificativ. Impactul este minim, riscul ca activitatea să nu se desfășoare normal este practic inexistent.

Incident de nivel major reprezintă o eroare apărută la o funcție sau proces, care afectează într-o mare măsură funcționarea întregului sistem de raportare on-line și/sau a website-ului. Poate avea impact asupra proceselor de business ale Beneficiarului. Există riscul ca incidentul să se extindă.

Incident de nivel critic reprezintă o eroare care afectează majoritatea funcționalităților sistemului de raportare on-line și/sau a website-ului sau a funcțiilor principale. Impact foarte mare asupra

mediului intern și extern. Risc mare privind: neexecutarea în termen a lucrărilor, deteriorarea imaginii Beneficiarului în relațiile cu Clienții acestuia.

Incident de nivel urgent reprezintă un incident de nivel critic pentru care nu există soluții alternative (workaround) care pot fi aplicate. Impact foarte mare asupra mediului intern și extern. Risc mare privind: neexecutarea în termen a lucrărilor, deteriorarea imaginii Beneficiarului în relațiile cu business-ul, pierderea imaginii pozitive a Beneficiarului în relația cu Clienții acestuia.

DIRECTOR DGO,

FLORIAN GRIGORE

DIRECTOR DTIS,


MIRCEA PASCU

ȘEF STI,

MARIUS DUMITRIU


Întocmit: Mihaela Dăescu
