

Instituția Prefectului - Județul Dolj  
Nr. 4024/31.03.2022

APROB  
SUBPREFECT  
Mariana-Venera Popescu

AVIZAT  
Șef Structură de Securitate  
Subprefect  
Nădăruș Popescu

Șef Serviciul Juridic  
Eugen Marinescu

## CAIET DE SARCINI privind achiziția de servicii de protecție informatică antivirus și anti-malware

### I. Obiectul achiziției, cantități

Prin prezentul *Caiet de Sarcini* se urmărește achiziționarea de servicii de protecție informatică antivirus și anti-malware pentru un număr de **54 stații de lucru și 3 servere** din cadrul Instituției Prefectului-Județul Dolj.

Achiziționarea serviciilor este necesară pentru asigurarea protecției împotriva virusurilor informatice și a software-ului de tip malware, spyware, spam, phishing și de altă natură, în măsură să afecteze securitatea și disponibilitatea stațiilor de lucru și serverelor din rețeaua locală și a stațiilor de lucru independente, pentru **perioada 01.05.2022 – 31.12.2022**.

### II: Cerințe minime obligatorii

#### II.1 Cerințe generale

Caietul de sarcini face parte din documentația de atribuire și constituie ansamblul criteriilor pe baza cărora se elaborează, de către fiecare ofertant, propunerea tehnică.

Toate cerințele din caietul de sarcini, inclusiv cerințele tehnice prezentate la punctul III, sunt minime și obligatorii.

#### **Oferta financiară:**

– se va prezenta în conformitate cu Formularul de ofertă și Anexa la Formularul de ofertă.

- valabilitatea ofertei: 30 de zile .

Criteriul de departajare este valoarea totală lei fără TVA.

Prețul cel mai scăzut/total servicii/ lei fără TVA, în condițiile respectării tuturor cerințelor din caietul de sarcini. Se ofertează toate serviciile.

#### **Oferta tehnică** va conține obligatoriu următoarele:

- Se va prezenta Oferta tehnică –descriere caracteristici tehnice produse.
- denumirea producătorului și a produsului pentru care se asigură serviciile ofertate;
- caracteristicile tehnice ale produsului care asigură îndeplinirea serviciilor de protecție
- nu se vor accepta ofertele vagi/generice sau alternative.

#### II.2 Condiții specifice de natură tehnică

Ofertele care nu respectă cumulativ cerințele tehnice de la punctul III vor fi respinse.

### III: Caracteristici tehnice ale produsului care asigură îndeplinirea serviciilor de protecție oferite

#### Caracteristici generale:

- să asigure protecție avansată în timp real antivirus, anti-malware, anti-spam, anti-spyware, anti-phishing, anti-ransomware, firewall

#### Modulul antivirus și anti-spyware:

- să asigure diferite niveluri de detecție bazată pe semnături, bazată de comportamentul fișierelor, pe monitorizarea proceselor.
- să aibă un singur motor de scanare bazat pe scanare automată în timp real, scanare în profunzime a arhivelor, euristică comportamentală, scanare bazată pe semnături, scanarea la cerere și la acces a oricărui mediu de stocare al informației, scanare automată a emailurilor atât la primire cât și la trimitere, scanare în rețea.
- să permită funcționarea și în modul standalone (cu sau fără suport de rețea)

#### Modulul anti-malware:

- să asigure protecție în timp real și filtrare contra website-uri malițioase
- să ofere protecție completă contra vulnerabilităților de sistem și software, astfel încât să nu fie exploatate de către un program malițios
- să asigure straturi multiple de protecție anti-ransomware cu rol de prevenire, detecție și remediere
- să monitorizeze procesele în timp real.

#### Modulul anti-spam:

- să permită funcția de filtrare a mesajelor de tip spam
- să permită funcția de scanare avansată anti-spam
- să se adapteze la noile tehnici de lansare a spam-ului

#### Modulul anti-phishing:

- să blocheze automat accesul la pagini web de tip phishing
- să detecteze trafic web și de rețea suspecte

#### Modulul actualizare:

- Actualizări de semnături de antivirus și anti-spyware periodice în mod automat și manual, protecție continuă împotriva celor mai noi amenințări informatice și upgrade la noile versiuni ale produsului pe perioada derulării contractului.

#### Modulul carantină:

- să trimită în carantină fișierele suspecte sau infectate printr-un mediu securizat care să nu afecteze funcționalitatea și disponibilitatea aplicațiilor care rulează în timp real pe stația de lucru și servere
- să șteargă automat fișierele carantinate mai vechi de o anumită perioadă
- să permită posibilitatea de restaurare și mutare a fișierelor din carantină în locațiile lor originale

#### Modulul administrare pentru stații de lucru și servere

- Consolele centrale de management vor facilita administrarea și instalarea agenților. După caz, soluția de virtualizare poate necesita una sau mai multe console pentru instalarea, configurarea, monitorizarea și raportarea stării de securitate a stațiilor de lucru și a serverelor.
- Consola de management trebuie să îndeplinească următoarele funcții minimale:
  - a. identificarea echipamentelor accesibile în rețea gruparea și gestionarea grupărilor de clienți antivirus pentru echipamentele din rețea;
  - b. identificarea stării echipamentelor din punctul de vedere al instalării soluției antivirus;
  - c. identificarea stării de activare globală și individuală a funcțiilor (activ/inactiv) și schimbarea acestora în funcție de necesități;
  - d. identificarea stării de actualizare și forțarea actualizării la nevoie;
  - e. gestionarea licențelor;
- Consola trebuie să aibă integrat un modul dedicat controlului activității utilizatorilor, cu următoarele funcții minimale:
  - a. restricționarea accesului la internet pentru anumiți clienți sau grupuri de clienți;
  - b. restricționarea accesului la internet pentru anumite aplicații;
  - c. restricționarea accesului la internet pentru anumite perioade de timp;
  - d. blocarea paginilor web care conțin anumite cuvinte cheie.
- Accesul la consola de management în urma introducerii credențialelor de acces (username și parolă).

Modulul rapoarte, grafice și alerte trebuie să asigure îndeplinirea următoarelor funcții:

- Crearea de rapoarte pe baza șabloanelor definite în consola de management.
- Generarea de rapoarte complete privind rezultatele scanării și infecțiilor detectate dar și a tuturor obiectelor scanate, inclusiv la nivelul clienților.
- Generarea în mod automat, în cazul detecției unui eveniment, a unui mesaj de alertă către una sau mai multe adrese de e-mail prin intermediul componentei centralizate.
- Generarea rapoartelor în mod programat și expedierea lor în mod automat prin e-mail către administrator.
- Generarea rapoartelor într-un format standardizat (ex.: html, pdf, etc.).

Capabilități:

- protecția mediilor de stocare de tipul USB/HDD, SSD, NVME, USB flash, CD/CD RW, DVD/DVD RW
- posibilitate blocare acces porturi citire/scriere a mediilor de stocare a stațiilor de lucru și servere
- posibilitatea de a oferi și de a utiliza o consolă centralizată de administrare, instalată local sau la distanță.
- Posibilitate detectare sandboxing

Compatibilitate:

- Prestatorul trebuie să asigure compatibilitatea cu sistemele de operare Windows 11, Windows 10 Professional, Windows 7 pentru stațiile de lucru și Windows Server Standard 2019 și Windows 2003 Server Enterprise Edition pentru servere, Mac, iPhone, iPad, Android.

În situația în care soluția generală nu poate acoperi un produs end-of-life solicităm o soluție compatibilă pentru Windows 2003 Server.

- Prestatorul trebuie să asigure compatibilitatea și integrabilitatea soluției de management centralizat cu Microsoft® Active Directory sistemele de operare Windows Server suportate.

Certificări:

- Să dețină cel puțin o certificare de specialitate emisă de organizații internaționale de profil (ex. Virus Bulletin, ICSA Labs, Checkmark)

#### IV: Specificații generale ale serviciilor suport

La solicitarea beneficiarului, prestatorul trebuie să fie în măsură să răspundă la incidentele provocate de atacuri ale virușilor sau al software-ului malițios în termen de 24 de ore, de la momentul semnalării evenimentului în cauză, ori prin deplasarea și intervenția în locația fizică a beneficiarului, dacă remedierea nu poate să fie realizată prin alte mijloace de asistență la distanță.

Prestatorul trebuie să fie în măsură să ofere un antidot pentru orice nou cod malițios semnalat de beneficiar în termen de cel mult 72 ore de la notificare.

Prestatorul trebuie să pună la dispoziție servicii de suport tehnic de instalare, configurare, diagnoză și remediere exclusiv în limba română, în regim 24/7, atât telefonic, cât și prin mijloace electronice (web, e-mail).

#### V: Condiții de plată

Plata contravalorii serviciilor prestate se va efectua lunar în termen de maxim 60 de zile de la data emiterii facturii și efectuarea recepției serviciilor.

Emiterea facturii se va face în termen de cel mult 7 zile de la sfârșitul lunii pentru care s-a efectuat prestarea serviciilor.

#### VI: Condiții de livrare, instalare și acceptanță

Instalarea și configurarea serviciilor trebuie să înceapă cât mai curând posibil, dar nu mai târziu de 7 zile calendaristice de la semnarea contractului și se va finaliza în termenul de instalare ce se va menționa în contract.

Acceptanța la beneficiar a instalării și configurării serviciilor va avea loc după încheierea tuturor procedurilor de instalare și configurare și întocmirea procesului verbal de acceptanță.

Prestatorul va pune la dispoziția beneficiarului pe suport optic/electronic toate kit-urile necesare, precum și documentația tehnică pentru instalarea, configurarea, administrarea și mentenanța serviciilor livrate.

Detalierea serviciilor de protecția informatică antivirus și antimalware este următoarea:

- serviciu de protecție informatică antivirus și antimalware pentru stații de lucru
- serviciu de protecție informatică antivirus și antimalware pentru servere

ÎNTOCMIT,  
Nigrini Mihai

Predea Claudia

## **ANEXA FORMULARE**

- Scrisoare de inaintare ( Formularul nr. 1 din anexa )
- Formularul de ofertă financiara si Anexa la Formularul de oferta
- Se va prezenta Oferta tehnica –descriere caracteristici tehnice produse.

OFERTANTUL

.....

(denumirea/numele)

Înregistrat la sediul autorității  
contractante.....

nr..... /.....

Ora \_\_\_\_\_

**SCRISOARE DE OFERTA**

Către,

.....  
(denumirea autorității contractante și adresa completă)

Ca urmare a anunțului din data de ..... privind achiziția directă pentru atribuirea contractului .....

noi ..... vă transmitem alăturat următoarele:

(denumirea/numele ofertantului)

- a) oferta financiara ;
- b) documentele care însoțesc oferta.

**2. Persoana de contact pentru achiziția directă**

Nume	
Adresă	
Telefon	
Fax	
E-mail	

Avem speranța că oferta noastră este corespunzătoare și va satisface cerințele.

Data completării .....

Operator economic,

.....

(semnătura autorizata și stampila)

OFERTANTUL \_\_\_\_\_ (denumirea/numele)

**FORMULAR DE OFERTĂ FINANCIARA**

Către,

**INSTITUȚIA PREFECTULUI DOLJ**

Str. Calea Unirii, nr. 19, 200585, Craiova, județul Dolj / Telefon 0251 414424 (6), 0251 416703 / Fax 0251 411210  
E-mail: [office@prefecturadolj.ro](mailto:office@prefecturadolj.ro) / Web site: <https://www.dj.prefectura.mai.gov.ro>

Doamnelor/Domnilor

1. Examinând documentația de atribuire directă, subsemnății, reprezentanți ai ofertantului \_\_\_\_\_, ne oferim ca, în conformitate cu prevederile și  
(denumirea/numele ofertantului)

cerințele cuprinse în documentația mai sus menționată, să furnizăm produsele, pentru suma de \_\_\_\_\_ lei (suma în litere și în cifre), la care se adaugă taxa pe valoarea adăugată în valoare de .....(suma în litere și în cifre).

2. Ne angajăm să menținem această ofertă valabilă pentru o durată de \_\_\_\_\_ zile, \_\_\_\_\_ (durata în litere și cifre), respectiv până la data de \_\_\_\_\_ (ziua/luna/anul), și ea va rămâne obligatorie pentru noi și poate fi acceptată oricând înainte de expirarea perioadei de valabilitate.

3. Până la încheierea și semnarea contractului această ofertă, împreună cu comunicarea transmisă de dumneavoastră, prin care oferta noastră este stabilită castigatorie, vor constitui un contract angajant între noi.

4. Precizăm ca:

nu depunem oferta alternativă.

depunem oferta alternativă.

Data \_\_\_\_/\_\_\_\_/\_\_\_\_

\_\_\_\_\_, în calitate de \_\_\_\_\_, legal autorizat să semnez  
(nume, semnătura)

oferta pentru și în numele \_\_\_\_\_.  
(denumirea/numele operator economic)

## OPERATORUL ECONOMIC

(denumirea/numele)

Centralizator preturi

Nr. crt	Denumirea serviciului	Cantitate	Preț unitar (Lei fără TVA)	Valoare lună (Lei fără TVA)	Valoare/ contract (lei, fără TVA)	Valoare totală contract cu TVA
0	1	2	3	4	5	7
1.	Pachet Serviciu de protecție informatică antivirus și antimalware pentru 54 stații de lucru	54				
2.	Serviciu de protecție informatică antivirus și antimalware pentru 3 servere	3				
<b>VALOARE TOTALĂ SERVICII CONTRACTATE</b>						
pentru perioada 01.05.2022 – 31.12.2022						

Notă:

**1. Rubrica "Cantitate" nu se va modifica!**

Data \_\_\_\_ / \_\_\_\_ / \_\_\_\_

\_\_\_\_\_, în calitate de \_\_\_\_\_, legal autorizat să semnez  
(nume/semnătură)

oferta pentru și în numele \_\_\_\_\_.  
(denumire/nume operator economic)