ANCPI
AGENȚIA NAȚIONALĂ DE CADASTRU ȘI PUBLICITATE IMOBILIARĂ

SECTIUNEA II - CAIET DE SARCINI

achiziție ”Servicii de protecție împotriva atacurilor cibernetice și a virușilor informatici”

1. Introducere

Caietul de sarcini face parte integrantă din Documentația de Atribuire și constituie ansamblul cerințelor pe baza cărora fiecare Ofertant va elabora Oferta (Propunerea Tehnică și Propunerea Financiară) pentru realizarea serviciilor care fac obiectul Contractului ce rezultă din această procedură.

Pentru scopul prezentei secțiuni a Documentației de Atribuire, orice activitate descrisă într-un anumit capitol din Caietul de Sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către Ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului Contractului.

Toate cerințele din prezentul caiet de sarcini, sunt minime și obligatorii, nerespectarea uneia dintre cerințe va duce automat la declararea ofertei ca fiind neconforma. Nu se acceptă depunerea de oferte alternative. Nu se admit ofertele parțiale din punct de vedere cantitativ și calitativ, ci numai ofertele integrale, care corespund tuturor cerințelor stabilite prin prezentul caiet de sarcini. Orice ofertă care se abate de la cerințele minimale va fi considerată admisibilă numai în condițiile în care aceasta asigură un nivel calitativ superior cerințelor minimale.

2. Contextul realizării acestei achiziții

2.1 Informații despre Autoritatea contractantă

În cadrul acestei proceduri, Agenția Națională de Cadastru și Publicitate Imobiliară îndeplinește rolul de Autoritate Contractantă, respectiv Achizitor în cadrul Contractului.

Potrivit Legii nr. 7/1996 a cadastrului și publicității imobiliare, republicată, cu modificările și completările ulterioare, Agenția Națională de Cadastru și Publicitate Imobiliară (ANCPI) este instituție publică, cu personalitate juridică, aflată în subordinea Ministerului Dezvoltării Regionale și Administrației Publice, unică autoritate în domeniile cadastru, publicitate imobiliară, geodezie, cartografie, fotogrammetrie și teledetecție.

Instituția are în subordine 42 de oficii teritoriale (OCPI) înființate în fiecare județ și municipiul București și Centrul Național de Cartografie (CNC) – instituții publice cu personalitate juridică. La rândul lor, oficiile coordonează birouri de cadastru și publicitate imobiliară (BCPI), existente în unități administrativ-teritoriale și altele decât reședințele de județ.

Scopul ANCPI este să poată furniza informații de calitate într-un mod eficient și transparent pentru toți cetățenii și să asigure o baza reala pentru dezvoltarea pieței imobiliare, a programelor guvernamentale si internaționale in domeniul cadastrului si publicității imobiliare.

2.2 Informații despre contextul care a determinat achiziționarea serviciilor

În scopul îndeplinirii atribuțiilor ce îi revin și pentru asigurarea unui serviciu public de calitate, în vederea eficientizării activității, standardizării proceselor, creșterii siguranței datelor administrate si controlului accesului la acestea, ANCPI dorește *achiziționarea serviciilor de suport tehnic, mentenanță și actualizare pentru soluția de securitate integrată* implementată în cadrul infrastructurii informatice proprii şi implementarea soluției existente pe echipamente noi ce fac obiectul unor achiziții recente. Serviciile se vor presta atât pentru ANCPI, cât şi pentru unităţile subordonate (42 OCPI-uri și CNC).

3. Descrierea serviciilor solicitate

3.1 Descrierea situației actuale la nivelul Autorității contractante

În prezent soluția de securitate implementată la nivelul ANCPI reprezintă o platforma integrată pentru managementul securității, este una unitară, omogenă, cu o consolă de management care asigură funcționalități de administrare, bazată pe soluția de protecție antivirus a producătorului Bitdefender, soluție pentru care există competențe de administrare solide la nivelul personalului tehnic al autorității contractante.

Soluția actuală de securitate din cadrul ANCPI s-a remarcat prin:

- management centralizat simplu și eficient
- rata de detecție a amenințărilor extrem de ridicată
- interfața în limba română
- suport disponibil prompt și în limba română
- furnizare rapidă de soluții (antidoturi) la noile amenințări apărute
- avertizări prin e-mail
- rata mică de alarme de tip "false-positive"
- permite instalarea personalizată a modulelor deținute
- integrare cu Active Directory
- include protecție împotriva atacurilor zero-day bazată pe machine learning (tehnologii de învățare automată)
- include un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil", proiectat special pentru a detecta atacuri avansate si activitati suspecte in faza pre-executie. Va proteja împotriva atacurilor directionate (Targeted Attack - APT), fisierelor suspecte si traficului la nivel de retea suspect, exploit-urilor, ransomware si grayware
- include un sandbox in cloud-ul public al producatorului acesteia, cu opțiunea de a trimite automat sau manual fișierele suspecte pentru a putea fi "detonate" spre a fi analizate în profunzime
- Posibilitatea de a actualiza din consolă sistemul de operare, precum și aplicațiile instalate pe stațiile de lucru
- Posibilitatea de a proteja datele stațiilor de lucru prin criptare din consolă
- impact minim asupra resurselor de procesare ale echipamentelor de generație mai veche pe care este instalată soluția.

3.1.1 Arhitectura sistemului

Această soluție este compusă din:

GravityZone Business Security Premium: consola de administrare plus agent de protecție antimalware și securitate – în prezent **pentru 3.800 utilizatori** (echipamente de tip endpoint).

3. Descrierea serviciilor solicitate

3.1 Descrierea situației actuale la nivelul Autorității contractante

În prezent soluția de securitate implementată la nivelul ANCPI reprezintă o platforma integrată pentru managementul securității, este una unitară, omogenă, cu o consolă de management care asigură funcționalități de administrare, bazată pe soluția de protecție antivirus a producătorului Bitdefender, soluție pentru care există competențe de administrare solide la nivelul personalului tehnic al autorității contractante.

Soluția actuală de securitate din cadrul ANCPI s-a remarcat prin:

- management centralizat simplu și eficient
- rata de detecție a amenințărilor extrem de ridicată
- interfața în limba română
- suport disponibil prompt și în limba română
- furnizare rapidă de soluții (antidoturi) la noile amenințări apărute
- avertizări prin e-mail
- rata mică de alarme de tip "false-positive"
- permite instalarea personalizată a modulelor deținute
- integrare cu Active Directory
- include protecție împotriva atacurilor zero-day bazată pe machine learning (tehnologii de învățare automată)
- include un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil", proiectat special pentru a detecta atacuri avansate si activitati suspecte in faza pre-executie. Va proteja împotriva atacurilor directionate (Targeted Attack - APT), fisierelor suspecte si traficului la nivel de retea suspect, exploit-urilor, ransomware si grayware
- include un sandbox in cloud-ul public al producatorului acesteia, cu opțiunea de a trimite automat sau manual fișierele suspecte pentru a putea fi "detonate" spre a fi analizate în profunzime
- Posibilitatea de a actualiza din consolă sistemul de operare, precum și aplicațiile instalate pe stațiile de lucru
- Posibilitatea de a proteja datele stațiilor de lucru prin criptare din consolă
- impact minim asupra resurselor de procesare ale echipamentelor de generație mai veche pe care este instalată soluția.

3.1.1 Arhitectura sistemului

Această soluție este compusă din:

GravityZone Business Security Premium: consola de administrare plus agent de protecție antimalware și securitate – în prezent **pentru 3.800 utilizatori** (echipamente de tip endpoint).

3.2 Obiectivul general la care contribuie

Soluția de securitate implementată la nivelul ANCPI este de importanță națională, a cărui eficiență este critică în ceea ce privește Strategia pentru Planul Național de Cadastru și Carte Funciară (PNCCF), sistemul integrat de cadastru și carte funciară E-Terra, angajamentele din cadrul programului EuroGeographics, raportarea în cadrul Directivei INSPIRE, serviciile puse la dispoziție către Registrele Agricole implementate la nivel Județean, Registrul Agricol Național, Registrul Electronic Național al Nomenclaturilor Stradale (RENNS) .

Fără asigurarea acestei necesități, riscurile nefuncționării sistemului informatic, funcționării cu întreruperi sau funcționării necorespunzatoare este major, având implicații directe asupra modului în care instituția poate să-și îndeplinească obiectivele asumate.

Obiectivul general la care contribuie prestarea serviciilor îl constituie protejarea sistemelor informatice din cadrul ANCPI, astfel ducând la îndeplinirea de către ANCPI a atribuțiilor ce îi revin și la asigurarea unui serviciu public de calitate, în vederea eficientizării activității, creșterii siguranței datelor administrate și controlului accesului la acestea.

3.3 Obiectivul specific la care contribuie prestarea serviciilor

Prin achiziția serviciilor de mentenanță pentru soluția integrată *de protecție împotriva atacurilor informatice și a virușilor informatici* descrise în prezentul document, Autoritatea Contractantă urmărește atingerea următoarelor obiective specifice:

- asigurarea unui nivel de securitate a sistemului informatic, în corelare cu importanța datelor și proceselor pe care le gestionează;
- accesul la asistență tehnică de specialitate;
- creșterea nivelului de protecție împotriva atacurilor cibernetice;
- funcționarea normală a aplicațiilor, pentru a permite desfășurarea corectă și continuă a activităților instituției;
- minimizarea sau eliminarea consecințelor datorate întreruperii funcționării sistemului sau funcționării defectuoase a acestuia.

3.4 Serviciile solicitate: activitățile ce vor fi realizate

Număr de utilizatori finali (endpoints): **minim 3.500, maxim 4.500.**

Serviciile de mentenanță pentru soluția integrată de *protecție împotriva atacurilor informatice și a virușilor informatici* vor include, pe întreaga perioadă a acordului cadru, următoarele activități:

- actualizarea bazei de semnături și a versiunilor soluției existente pentru managementul securității
- suport și asistență tehnică de specialitate on-line și/sau on-site
- transfer de cunoștințe (dacă este cazul)

- auditare tehnică periodică a stării de funcționare a soluției integrate de protecție împotriva atacurilor informatice și a virușilor informatici.

Performanțele și capabilitățile tehnice ale soluției oferite vor fi cel puțin egale cu cele ale soluției deținute de beneficiar și va asigura în mod minimal performanțele și capabilitățile precizate mai jos:

- management centralizat prin consolă folosind doar accesul securizat HTTPS;
- interfața în limba română;
- suport disponibil prompt și în limba română;
- furnizare rapidă de soluții (antidoturi) la noile amenințări apărute;
- avertizări prin e-mail, SMS etc.
- mecanisme pentru diminuarea ratei de alarme de tip "false-positive";
- mecanisme de invatare (maschine learning);
- mecanisme de analiza externa a fisierelor suspecte;
- impact redus asupra resurselor de procesare ale echipamentelor;
- compatibilitate cu Windows 7 sau superior, pe 32 si 64 bites;
- compatibilitate Mac OS Sierra sau superior;
- compatibilitate Windows server 2008 R2 sau superior;
- Protecție împotriva atacurilor cibernetice de tipul:
  - Exploatări;
  - Viruși, viermi și cai troieni;
  - Atacuri pe bază de script;
  - Ransomware și grayware;
  - Atacuri fără fișiere;
  - Phising;
  - Malware necunoscut;
  - Atacuri ascunse;
  - etc.
- Antiexploatare și hiperdetecție (machine learning);
- Sandbox;
- Securitate web și Anti-Phishing;
- Modul de detectare, corelare și răspuns la evenimente de tip EDR („endpoint detection and response") capabil să identifice amenințări avansate sau atacuri în curs de desfășurare;
- Modul de tip host IPS capabil să blocheze atacuri la nivel de rețea incluzând mișcarea laterală a unor categorii de malware;
- Firewall client;
- Carantina – fișierele suspecte și infectate vor fi trimise in carantină pentru o anumită perioadă, cu posibilitatea recuperării acestora;
- Controlul conținutului: blocare acces internet pentru anumiți clienți, în anumite intervale orare, acces anumite programe la internet, acces numai la anumite pagini de internet;
- Controlul dispozitivelor: permite controlul dipozitivelor de tipul: usb, floppy, cd-dvdrom, network adapters, tape drives, printers etc;
- Power User: utilizatorii vor putea accesa și modifica setările clientului malware local;
- Soluția antimalware trebuie să aibă 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișierelor și bazată pe monitorizarea proceselor;
- Soluția va dispune de un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat de pe internet, fără intervenția administratorului;

- Se va permite definirea de locații de actualizare multiple;
- Se va permite actualizarea intr-o rețea fără acces la internet;
- Integrare cu Active Directory, Vmware vCenter;
- Inventariere stații fizice neintegrate in Active Directory; Se permite descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM;
- Soluția va permite selectarea modulelor componente atunci cand se crează pachetul clientului care se instalează pe mașinile fizice/virtuale, iar instalarea va fi permisă la distanță sau manual;
- Soluția va permite configurarea centralizată a clientilor antimalware prin intermediul politicilor;
- Politica va conține opțiuni specifice de activare/dezactivare și configurarea functionalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, scanarea traficului web, controlul dispozitivelor, power user, sandbox in cloud, modul avansat bazat pe tehnologii de tip machine-learning tunabil, modul de tip Endpoint-Detection and Response (EDR).
- Soluția va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antimalware, precum si posibilitatea de repornire a mașinilor;
- Soluția va conține rapoarte care prezintă statusul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate. Va fi inclus un generator de rapoarte care oferă informații ordonate, în baza mai multor criterii. Rapoartele vor fi exportate in format pdf si csv;
- Soluția va permite administratorului să efectueze „call-uri" API
- Posibilitatea de a actualiza din consolă sistemul de operare, precum și aplicațiile instalate pe stațiile de lucru;
- Posibilitatea de a proteja datele stațiilor de lucru prin criptare din consolă;

3.4.1 Servicii de actualizare a bazei de semnături și a versiunilor soluției antivirus

Cerințele pentru serviciile de actualizare a bazei de semnături și a versiunilor pentru soluția de protecție sunt :

- actualizarea automată/manuală a software-ului, cu titlu gratuit, la cele mai noi versiuni disponibile. Actualizarea va ține cont de platforma hardware pe care o deține Achizitorul;
- actualizarea automată a bazei de date de semnături;

3.4.2 Servicii de suport și asistență tehnică de specialitate on-line și/sau on-site

1. Prestatorul va asigura accesul la un serviciu de tip call-center în urmatoarele condiții:
   a. forma de comunicare:
      - telefon;
      - e-mail;
      - portal tehnic Prestator;
      - suport tehnic online – Baza de cunostințe (Knowledge Base);
      - noutăți tehnice (newsletter) prin email;
      - chat.
   b. Disponibilitate: 24 ore pe zi, 7 zile pe săptămână (cel puțin una dintre formele de comunicare stabilite)

2. Intervenții on-line sau on-site

La solicitare, Prestatorul va pune la dispoziția Beneficiarului - personal de specialitate pentru intervenții și/sau analize tehnice on-line sau on-site, în funcție de situație.

În cazul în care este aplicabil, la solicitarea Beneficiarului, experții desemnați ai Prestatorului vor accesa la distanță (remote) sistemele Beneficiarului / se vor deplasa în sediul central al Beneficiarului, pe baza drepturilor de acces acordate, în vederea îndeplinirii unor activități specifice:

- analize de impact;
- configurări și reconfigurări ale componentelor soluției implementate;
- servicii de auditare tehnică periodică a stării de funcționare a soluției;
- analize ale vulnerabilităților și riscurilor.

Intervenția se va face în minim 24 ore de la data solicitării, cu excepția zilelor libere legale, începând cu prima zi lucrătoare.

3. Vor trebui onorate, la timp și la nivelul cerut de parametrii de calitate, toate acele solicitări venite din partea personalului specializat în tehnologia informației desemnați de Autoritatea contractantă către specialiștii tehnici desemnați din partea prestatorului, cu respectarea următorilor timpi de intervenție: timp de răspuns: 1 oră; timp de implementare soluție provizorie 4-8 ore; timp de remediere 24-48h.

Rezultatele intervențiilor vor fi consolidate în rapoarte tehnice însoțite de recomandări menite să elimine sau să diminueze vulnerabilitățile și/sau efectele unor atacuri.

3.5 Rezultatele care trebuie obținute în urma prestării serviciilor

Implementarea Contractului în conformitate cu prevederile prezentului Caiet de Sarcini trebuie să conducă cel puțin la atingerea următoarelor rezultate finale măsurabile:

- rezolvarea problemelor apărute în sistem, pentru evitarea impactului în derularea operațiunilor zilnice;
- nivel ridicat de protecție la atacurile cibernetice;
- protecția datelor și echipamentelor;
- continuitate în funcționare prin acces la asistența tehnică de specialitate
- funcționarea normala a aplicațiilor, pentru a permite desfășurarea corectă și continuă a activităților instituției ;
- minimizarea sau eliminarea consecințelor datorate întreruperii funcționării sistemului sau funcționării defectuoase a acestuia.

3.6 Atribuțiile și responsabilitățile Părților

3.6.1 Atribuțiile și responsabilitățile Autorității Contractante

Autoritatea Contractantă este responsabilă pentru:

- punerea la dispoziția Prestatorului a tuturor informațiilor disponibile pentru obținerea rezultatelor așteptate, cum ar fi: date de intrare, raportări, situații specifice;
- punerea la dispoziția Prestatorului, dacă și când este cazul, a unui spațiu de lucru adecvat;
- desemnarea echipei implicate și responsabile cu interacțiunea și suportul oferit Prestatorului;
- asigurarea tuturor resurselor care sunt în sarcina sa pentru buna derulare a Contractului;

- desemnarea responsabilului pentru derularea acordului cadru și a contractelor subsecvente atribuite în baza acestuia;
- efectuarea plaților în conformitate cu prevederile contractuale.

3.6.2 Atribuțiile și responsabilitățile Prestatorului

Prestarea serviciilor menționate la punctul *3.4. Servicii de protecție împotriva atacurilor informatice și a virușilor informatici* se va face **pe bază de abonament lunar/ trimestrial**, în funcție de durata contractului subsecvent încheiat (pe o lună sau mai multe), fără alte costuri suplimentare pentru Autoritatea Contractantă.

Prestatorul are obligația să presteze serviciile contractate în următoarele condiții:

- Operaționalizarea unui serviciu de tip „help-desk" telefonic, email sau sesiune remote cu personal calificat pentru preluarea, clasificarea și distribuția tichetelor de suport, cu program:
  - 24 ore x 7 zile pe săptămână;
  - În intervalul 08:00-18:00, în zilele lucrătoare, pentru severități inferioare celei maxime.
- asigurarea planificării resurselor în raport cu termenele stabilite pentru derularea contractelor subsecvente atribuite în baza acordului-cadru;
- îndeplinirea obligațiilor sale, cu respectarea celor mai bune practici din domeniu, a prevederilor legale și contractuale relevante, precum și cu deplina înțelegere a complexității legate de derularea cu succes a acordului-cadru, astfel încât să se asigure îndeplinirea obiectivelor stabilite;
- asigurarea valabilității tuturor autorizațiilor și certificatelor (atât pentru organizația sa, cât și pentru personal), care sunt necesare (conform legislației în vigoare) pentru implementarea contractelor subsecvente atribuite în baza acordului-cadru;
- îndeplinirea obligațiilor contractuale în conformitate cu cerințele Caietului de Sarcini;
- colaborarea cu personalul Autorității contractante alocat pentru derularea și implementarea contractelor subsecvente (coordonarea activităților, intervenții în timpii solicitați);
- asigurarea personalului adecvat (din punct de vedere al calificării educaționale și profesionale), ca și infrastructura/echipamentele necesare pentru efectuarea eficientă a tuturor activităților enumerate în Caietul de Sarcini și pentru realizarea obiectivului stabilit prin contractele subsecvente atribuite în baza acordului-cadru;
- asigurarea în permanență a disponibilității resurselor umane/materiale necesare;
- numirea persoanei responsabile cu derularea acordului-cadru și a contractelor subsecvente înainte de atribuirea primului contract subsecvent;
- atenționarea autorității contractante asupra oricărui element care poate să pună în pericol îndeplinirea la timp și corespunzătoare a unei activități.

4. Ipoteze și riscuri

Prestatorul acționează în interesul Autorității Contractante pe durata prestării serviciilor solicitate, în condițiile și cu limitele descrise în documentația aferentă prezentei proceduri de atribuire.

Prestatorul acționează în sensul realizării obiectivelor prezentate pentru Contract în ceea ce privește optimizarea folosirii resurselor necesare îndeplinirii obiectivelor prezentului Caiet de Sarcini.

4.8 Ipoteze

În vederea derulării activităților și etapelor prevăzute de contract, sunt luate în considerare următoarele ipoteze:

- nu se prevăd schimbări ale cadrului instituțional și legal care să afecteze major implementarea și desfășurarea în bune condiții a Contractului;
- toate informațiile relevante și disponibile la nivelul Autorității Contractante pentru realizarea serviciilor vor fi puse la dispoziția Contractantului;

4.9 Riscuri

4.9.1 Riscuri identificate de Autoritatea Contractantă în perioada de implementare a contractelor subsecvente

RISC	CONSECINȚE	MĂSURI DE DIMINUARE
Dificultăți de colaborare și comunicare între părțile contractante	Întârzieri în rezolvarea problemelor tehnice reclamate de autoritatea contractanta	Părțile vor desemna persoanele responsabile pentru implementarea contractelor subsecvente înainte de atribuirea primului contract subsecvent.
Calitatea serviciilor și/sau performanța Prestatorului sunt necorespunzătoare	Servicii de calitate necorespunzătoare, implementarea cu întârziere a proiectului, dispute contractuale	Stabilirea de cerințe referitoare la experiența și calificarea personalului. Clauze contractuale care permit Autorității Contractante să solicite schimbarea unui membru al echipei Prestatorului dacă acesta are o activitate necorespunzătoare.
Contractorul nu își îndeplinește obligațiile contractuale la timp / își încetează activitatea	Întârzieri în asigurarea funcționalității sistemului în parametrii normali	Stabilirea de clauze contractuale penalizatoare prin care să se poată gestiona situațiile de neîndeplinire/ îndeplinire cu întârziere a obligațiilor; Participarea operatorului economic cu un terț susținător pentru transferul responsabilităților de prestare servicii.

4.9.2 Riscuri identificate de Candidați

De asemenea, pe lângă riscurile de mai sus, ofertanții vor identifica și alte riscuri asociate derulării contractelor subsecvente de prestări de servicii pe care le vor prezenta în cadrul propunerii tehnice, pe modelul tabelului de mai sus.

Analiza detaliată a riscurilor va fi întocmită, în perioada de tranziție, de Ofertantul declarat câștigător.

5. Abordare și metodologie în cadrul Contractului

5.8 Timpi de intervenție – SLA (Service Level Agreement)

În funcție de gradul de severitate, prestatorul trebuie să preia sesizările transmise în intervalul orar stabilit și să furnizeze soluții cu respectarea următorilor **timpi de intervenție (SLA):**

- timp de preluare sesizare (confirmare): 1 oră;
- timp de remediere defecțiune pe grade de severitate:
  1. **Critică – 2 ore**
  2. **Majoră – 8 ore**
  3. **Medie – 24 ore**
  4. **Mică – 48 ore**

Pentru o înțelegere corectă a termenilor folosiți în prezentul Caiet de Sarcini vor fi luate în considerare definiția:

- **Defecțiune** – situație care apare în exploatarea sistemului cauzată de atacuri informatice sau/și viruși informatici și care pot afecta utilizarea acestuia total sau parțial.

5.1 Program de disponibilitate

Pentru nivele de severitate critică și majoră – programul de disponibilitate este 24 ore din 24, 7 zile din 7.

Pentru nivele de severitate medie și mică – intervenția se va face în intervalul 08:00-18:00, în zilele lucrătoare, cu excepția zilelor libere legale, începând cu prima zi lucrătoare.

6. Plan de lucru pentru activitățile/serviciile solicitate

1. Prestatorul va asigura accesul la un serviciu de tip call-center în urmatoarele condiții:
   a. forma de comunicare:
      - telefon;
      - e-mail;
      - portal tehnic Prestator;
      - suport tehnic online – Baza de cunostințe (Knowledge Base);
      - noutăți tehnice (newsletter) prin email;
      - chat.
   b. Disponibilitate: 24 ore pe zi, 7 zile pe săptămână (cel puțin una dintre formele de comunicare stabilite)

2. *Intervenții on-line sau on-site*

La solicitare, Prestatorul va pune la dispoziția Beneficiarului - personal de specialitate pentru intervenții și/sau analize tehnice on-line sau on-site, în funcție de situație.

La solicitarea beneficiarului prestatorul va face auditare tehnică a stării de funcționare a soluției integrate de protecție împotriva atacurilor informatice și a virușilor informatici, cel puțin o dată pe an. Rezultatele acetei auditări se vor regăsi în Raportul de activitate aferent acelei perioade.

În cazul în care este aplicabil, la solicitarea Beneficiarului, experții desemnați ai Prestatorului vor accesa la distanță (remote) sistemele Beneficiarului / se vor deplasa în sediul central al Beneficiarului, pe baza drepturilor de acces acordate, în vederea îndeplinirii unor activități specifice:

- analize de impact;
- configurări și reconfigurări ale componentelor soluției implementate;
- servicii de auditare tehnică periodică a stării de funcționare a soluției;
- analize ale vulnerabilităților și riscurilor.

3. Vor trebui onorate, la timp și la nivelul cerut de parametrii de calitate, toate acele solicitări venite din partea personalului specializat în tehnologia informației desemnați de Autoritatea contractantă către specialiștii tehnici desemnați din partea prestatorului, cu respectarea timpilor de intervenție de la ***pct. 5.2 – Timpi de intervenție (SLA).***

Rezultatele intervențiilor vor fi consolidate într-un **Raport de activitate** însoțit de recomandări menite să elimine sau să diminueze vulnerabilitățile și/sau efectele unor atacuri.

7. Locul și durata desfășurării activităților

7.1 Locul desfășurării activităților

Activitățile de mentenanță se vor desfășura la sediul Prestatorului.

Pentru desfășurarea de către Prestator a activităților ce decurg din prezentul Caiet de Sarcini, Autoritatea Contractantă va asigura acces „de la distanță" la sistem, în conformitate cu politica sa de securitate.

Autoritatea Contractantă își rezervă dreptul de a solicita prezența experților Prestatorului la sediul ei, atunci când consideră că este necesar.

7.2 Durata prestării serviciilor

Agenția Națională de Cadastru și Publicitate Imobiliară va încheia un **Acord Cadru pentru o perioadă de 48 de luni**, în urma organizării procedurii de achiziție.

8. Resursele necesare/expertiza necesară pentru realizarea activităților în Contract și obținerea rezultatelor

Prestatorul trebuie să se asigure că personalul care își desfășoară activitatea în cadrul Contractului, dispune de sprijinul material și de infrastructura necesară pentru a permite acestuia să se concentreze asupra realizării activităților din cadrul Contractului.

9. Cadrul legal care guvernează relația dintre Autoritatea Contractantă și Prestator

Prestatorul are obligația de a respecta în executarea Contractului, obligațiile aplicabile în domeniul mediului, social și al muncii instituite prin dreptul Uniunii, prin dreptul național, prin acorduri colective sau prin dispozițiile internaționale de drept în domeniul mediului, social și al muncii.

Pe perioada realizării tuturor activităților din cadrul contractelor subsecvente, Prestatorul este responsabil pentru implementarea celor mai bune practici, în conformitate cu legislația și regulamentele existente la nivel național și la nivelul Uniunii Europene. Prestatorul va fi ținut deplin responsabil pentru subcontractanții săi în prestarea serviciilor prevăzute în Caietul de Sarcini, urmând să răspundă față de Autoritatea Contractantă, pentru orice nerespectare sau omisiune a respectării oricăror prevederi legale și normative aplicabile.

Autoritatea Contractantă nu va fi ținută responsabilă pentru nerespectarea sau omisiunea respectării de către Prestator sau de către subcontractanții acestuia a oricărei prevederi legale sau a oricărui act normativ aplicabil precum și atât pentru prestarea serviciilor cât și pentru rezultatele generate de prestarea serviciilor.

În cazul în care intervin schimbări legislative, Prestatorul are obligația de a informa Autoritatea Contractantă cu privire la consecințele asupra activităților care fac obiectul Contractului și de a-și adapta activitatea în funcție de decizia Autorității Contractante în legătură cu schimbările legislative.

Prestatorul și subcontractanții propuși vor prezenta ca anexă la propunerea tehnică câte o declarație privind respectarea reglementarilor obligatorii din domeniul mediului, social, al relațiilor de munca si privind respectarea legislației de securitate si sănătate in munca.

Informații suplimentare pot fi obținute de la instituțiile abilitate, respectiv:

- Ministerul Mediului, Apelor și Pădurilor, Bld. Libertății nr. 12, Sector 5, București, Romania, Tel. +40 21 408 9605, Fax: +40 21 408 9615, Adresa internet (URL): http://www.mmediu.ro.

- Ministerul Muncii si Protecției Sociale str. Dem.I.Dobrescu nr.2-4 sectorul 1, București, Romania, Tel. +40 213136267, Fax: +40 213136267, Adresa internet (URL): www.mmuncii.ro.

Ofertantul si, daca este cazul, subcontractanții, au obligația de a prezenta anexat propunerii tehnice o declarație pe propria răspundere prin care se va certifica ca serviciile prestate nu încalcă dreptul de proprietate intelectuala (brevete, nume, mărci înregistrate, patente, licențe, desene, modele, etc.) aparținând unui terț.

Ofertanții si, daca este cazul, subcontractanții, au obligația de a prezenta o declarație pe proprie răspundere din care sa rezulte ca, pe perioada de implementare a contractelor subsecvente ce vor fi atribuite in baza acordului-cadru, vor respecta prevederile Regulamentului nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date. În cadrul acestei declarații, Ofertantul sau persoana imputernicită își asumă că toți experții care au depus CV în cadrul ofertei, au fost de acord cu prelucrarea datelor cu caracter personal.

La momentul semnării acordului-cadru, sau după caz, la momentul implicării în proiect, Prestatorul și echipa sa (experții principali, experți secundari, și orice alte persoana care intră în contact cu datele sistemului supus mentenanței) vor semna fiecare un acord/declarație de confidențialitate asupra datelor cu care vor intra în contact pe perioada derulării acordului-cadru și vor respecta toate instrucțiunile privind utilizarea informațiilor confidențiale.

10. Managementul/Gestionarea Contractului și activități de raportare în cadrul Contractului

10.1 Gestionarea relației dintre Prestator și Autoritatea Contractantă

În vederea gestionării relației dintre Prestator și Autoritatea Contractantă, în cadrul celei din urmă va fi desemnat un responsabil de contract.

10.2 Rapoartele/documentele solicitate de la Prestator

În termen de maxim 3 zile lucrătoare de la sfârșitul perioadei de prestație, Prestatorul va transmite responsabilului de contract al Achizitorului un **Raport de activitate** (lunar sau trimestrial), în care va consemna, pentru perioada de prestație aferentă, următoarele :

- Lista sesizărilor transmise de Achizitor și modalitatea de soluționare, timpul de soluționare;
- Rapoarte de incident, însoțite de analiza cauzelor și recomandări privind acțiunile necesare reducerii riscului de recidivă;

Raportul de activitate va fi verificat de responsabilul de contract al Autorității Contractante. În cazul unor neconformități de formă, acesta poate solicita prestatorului, printr-o notificare scrisă, remedierea acestora.

Prestatorul va remedia neconformitățile semnalate și va transmite o nouă versiune a raportului în max. 5 zile lucrătoare de la data primirii notificării.

Forma și structura raportului va fi stabilită și adoptată de reprezentanții celor doua părți, imediat după semnarea primului contract subsecvent.

10.3 Acceptanța serviciilor

Raportul de activitate, menționat la **pct. 10.2**, va fi verificat și adoptat de responsabilul de contract din partea Autorității Contractante, într-un termen cuprins între 5 și 10 de zile lucrătoare, în funcție de complexitatea raportului.

În cazul constatării unor neconformități, responsabilul de contract al Autorității contractante va solicita Prestatorului, printr-o notificare scrisă, remedierea acestora. Prestatorul va transmite, în termenul precizat în notificare (nu mai mult de 5 zile lucrătoare), o nouă versiune revizuită a Raportului de mentenanță corectivă și de întreținere.

Responsabilul de contract din partea Autorității Contractante va verifica Raportul de activitate revizuit in termen de maximum 3 zile lucrătoare, iar în cazul în care se constată din nou neconformități, serviciile se consideră întârziate și se aplică penalități conform clauzelor contractuale.

Serviciile prestate sunt considerate acceptate și pot fi plătite doar dacă pentru acestea, Autoritatea Contractantă a emis un certificat de acceptanță. Certificatul de acceptanta va fi emis de responsabilul de contract numit prin ordin al directorului general al entității achizitoare, în termen de maxim 5 zile lucrătoare. Termenul se calculează de la data primirii documentelor prevăzute, în funcție de tipul de livrabil.

10.4 Finalizarea serviciilor în cadrul Contractului

Autoritatea Contractantă va considera serviciile din cadrul Contractului finalizate în momentul în care:

a) toate cerințele cuprinse în Caietul de Sarcini au fost îndeplinite;
b) toate obligațiile contractuale au fost îndeplinite.

La finalizarea fiecărui contract subsecvent Autoritatea Contractantă va emite un Document constatator în conformitate cu prevederile legale în vigoare în materie de achiziții publice.

10.5 Efectuarea plăților în cadrul Contractului

Plata serviciilor de *protecție împotriva atacurilor informatice și a virușilor informatici* se va face trimestrial, sau lunar în cazul contractelor subsecvente încheiate pe o perioadă mai mică de 3 luni, prin OP, în contul de trezorerie al Prestatorului, în termen de 30 de zile de la data înregistrării facturii electronice în sistemul național privind factura electronică RO e-Factura, în conformitate cu dispozițiile legale în vigoare, emisă de Prestator. Prestatorul va emite factura după emiterea de către Autoritatea contractantă, prin reprezentanții desemnați în acest sens, a certificatului de acceptanță.

10.6 Penalități pentru întârzieri în prestarea serviciilor

Depășirea termenelor limită de intervenție stabilite, se penalizează cu un punct de penalitate pentru fiecare oră de întârziere. Fracțiunile de ora se rotunjesc la o ora. Un punct de penalitate reprezintă un cuantum financiar 0.02% din valoarea, fără TVA, aferentă perioadei de raportare.

Pentru neîndeplinirea celorlalte obligații contractuale sau alte întârzieri în îndeplinirea serviciilor, prestatorul va plăti ca penalitate un procent de 0,05% din valoarea, fără TVA, aferentă perioadei de raportare.

Penalitățile se deduc din valorile contractuale – fără TVA - aferente perioadei de raportare, pe baza raportului de activitate, fără a se depăși valoarea totală aferentă perioadei de raportare.

În cazul în care se înregistrează penalități mai mari de 10% din valoarea aferentă unei perioade de raportare, în două intervale de raportare consecutive, autoritatea contractantă poate rezilia unilateral contractul.

În cazul în care se înregistrează penalități mai mari de 30% din valoarea aferentă unei perioade de raportare, autoritatea contractanta poate rezilia unilateral contractul.

11. Criteriul de atribuire

În cadrul acestei proceduri de achiziție – licitație deschisă, criteriul de atribuire „prețul cel mai mic" este criteriul care răspunde în mod echitabil necesității Autorității Contractante.