



Cofinanțat de
Uniunea Europeană



CAIET DE SARCINI

*pentru achiziția de “Sistem de protecție pentru soluția de mesagerie electronică” pentru
extinderea capacității de apărare cibernetică împotriva amenințărilor specifice
serviciilor de poștă electronică în site-ul DR/BC, în cadrul proiectului MAI Digital, cod
SMIS 318777*

1. INTRODUCERE

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

Caietul de sarcini conține, în mod obligatoriu, specificații tehnice, care vor fi considerate ca fiind minimale. Acestea definesc, după caz și fără a se limita la cele ce urmează, caracteristici referitoare la nivelul calitativ, tehnic și de performanță, siguranța în exploatare, dimensiuni, precum și sisteme de asigurare a calității, terminologie, simboluri, teste și metode de testare, ambalare, etichetare, marcare, condițiile pentru certificarea conformității cu standarde relevante sau altele asemenea.

În acest sens, orice ofertă cu caracteristici tehnice inferioare celor prevăzute în caietul de sarcini sau care nu satisface toate aceste cerințe va fi declarată neconformă și va fi respinsă. Nu se acceptă depunerea de oferte alternative.

Caietul de sarcini precizează și instituțiile competente de la care furnizorii, executanții sau prestatorii pot obține informații privind reglementările obligatorii referitoare la protecția muncii, la prevenirea și stingerea incendiilor și la protecția mediului, care trebuie respectate pe parcursul îndeplinirii contractului și care sunt în vigoare la nivel național.

În cadrul acestei proceduri, Ministerul Afacerilor Interne prin Direcția Achiziții Publice îndeplinește rolul de Autoritate contractantă, în cadrul Contractului.

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.

În conformitate cu prevederile legale în vigoare privind achizițiile publice, orice specificație tehnică menționată în prezentul caiet de sarcini/anexe se înțelege a fi însoțită de mențiunea „sau echivalent”, dacă este cazul.

În propunerea tehnică Ofertanții trebuie să precizeze concis marca, denumirea/modelul/versiunea/part-number-ul produsului, așa cum figurează la producător și specificațiile tehnice ale acestuia care îndeplinesc cerințele minime din prezentul Caiet de sarcini.

Conformitatea produselor se va justifica pe bază de publicații (materiale oficiale, disponibile public și accesibile în mod liber și gratuit de către Autoritatea contractantă, în scop de verificare) și/sau confirmări explicite ale producătorilor respectivi (oferite în original sau în copie conform cu originalul) incluse în ofertă.

2. CONTEXTUL REALIZĂRII ACESTEI ACHIZIȚII

Obiectul procedurii constă în atribuirea unui contract pentru achiziția și furnizarea unui sistem de protecție pentru soluția de mesagerie electronică, destinate extinderii

capabilității de apărare cibernetică împotriva amenințărilor specifice serviciilor de poștă electronică în site-ul Disaster Recovery și Business Continuity (DR/BC), în cadrul proiectului MAI Digital, cod SMIS 318777.

2.1. Informații despre Autoritatea contractantă

Autoritatea contractantă este Ministerul Afacerilor Interne, instituție din sistemul de apărare, ordine publică și siguranță națională. Ministerul Afacerilor Interne este organ de specialitate al administrației publice centrale, cu personalitate juridică.

Direcția Generală pentru Comunicații și Tehnologia Informației din Ministerul Afacerilor Interne (MAI) va asigura în numele Autorității contractante relaționarea pe timpul derulării procedurii de achiziție și operaționalizării Sistemului de protecție pentru soluția de mesagerie electronică, dedicat, pentru extinderea capabilității de apărare cibernetică împotriva amenințărilor specifice serviciilor de poștă electronică în site-ul DR/BC.

2.2. Informații despre contextul care a determinat achiziționarea produselor și serviciilor

Prezența achiziție este determinată de necesitatea asigurării continuității serviciilor de mesagerie electronică, precum și a capacității de recuperare în caz de dezastru pentru infrastructura aferentă.

În acest context, site-ul Disaster Recovery și Business Continuity (DR/BC) va fi dotat cu soluții tehnice compatibile și interoperabile cu sistemele existente, în vederea extinderii capabilităților de apărare cibernetică împotriva amenințărilor specifice serviciilor de poștă electronică, precum și pentru asigurarea funcționării în regim redundant, a unui management unitar, a unei mentenanțe eficiente și a standardizării configurațiilor de securitate.

Sistemul ce urmează a fi achiziționat va include echipamente hardware dedicate de tip email gateway security și sandbox hardware, licențiate și dimensionate corespunzător, împreună cu subscripțiile necesare funcționării, destinate protecției fluxurilor de poștă electronică.

Aceste echipamente vor fi integrate cu infrastructura existentă din site-ul principal, respectiv cu platforma de securitate pentru mesagerie electronică deja implementată, organizată în cluster redundant, asigurând interoperabilitate completă, funcționare unitară, sincronizarea politicilor de securitate și corelarea mecanismelor de detecție și răspuns la amenințări.

Soluția ofertată trebuie să asigure integrarea fără afectarea funcționării infrastructurii existente.

Ofertantul va demonstra în cadrul propunerii tehnice modalitatea concretă de integrare a soluției ofertate cu infrastructura existentă, inclusiv mecanismele de interoperabilitate, sincronizare a politicilor de securitate și schimb de informații privind amenințările.

2.3. Informații despre beneficiile anticipate de către Autoritatea contractantă

Prin această achiziție se va asigura implementarea și menținerea unui nivel adecvat de securitate și continuitate a serviciilor IT critice, în special a serviciilor de mesagerie electronică, în conformitate cu cerințele privind continuitatea activității și recuperarea în caz de dezastru (DR/BC).

Totodată, achiziția contribuie la extinderea capabilităților de protecție a serviciilor de mesagerie electronică la nivelul site-ului Disaster Recovery și Business Continuity (DR/BC), asigurând replicarea și funcționarea în condiții de siguranță a infrastructurii de e-mail în scenarii de avarie sau indisponibilitate a infrastructurii principale.

Sistemul de protecție pentru soluția de mesagerie electronică va permite asigurarea unei protecții avansate a fluxurilor de e-mail, prin utilizarea mecanismelor de filtrare antispam și antivirus, precum și prin analiza comportamentală a fișierelor și atașamentelor suspecte, în vederea identificării și blocării amenințărilor informatice avansate.

Implementarea acestor echipamente în site-ul DR/BC va contribui la creșterea rezilienței infrastructurii de mesagerie electronică, la reducerea riscului de compromitere a sistemelor informatice și la prevenirea incidentelor de securitate care pot afecta disponibilitatea și integritatea serviciilor de poștă electronică.

De asemenea, soluția trebuie să fie corelată cu subscripțiile existente la nivelul infrastructurii din site-ul principal, astfel încât să fie evitate decalajele între perioadele de licențiere și să se asigure continuitatea serviciilor de securitate fără întreruperi sau degradări de funcționalitate.

Soluția va asigura funcționarea unitară cu infrastructura existentă, inclusiv din perspectiva politicilor de securitate și a mecanismelor de detecție și răspuns la amenințări.

2.4. Alte inițiative /proiecte/programe asociate cu această achiziție de produse și servicii

Pentru asigurarea suportului tehnic de infrastructură și comunicații necesar tuturor structurilor MAI cu responsabilități specifice în domeniul operativ, coroborat cu necesitatea asigurării unui climat de securitate optim pentru serviciile publice electronice furnizate de către MAI prin intermediul portalului hub.mai.gov.ro și al altor platforme informatice instituționale, este necesară **operaționalizarea site-ului Disaster Recovery și Business Continuity (DR/BC)** și extinderea infrastructurii aferente serviciilor IT critice.

În acest context, prezenta achiziție are ca scop extinderea serviciilor de poștă electronică în site-ul DR/BC, prin implementarea unor soluții dedicate de securitate pentru infrastructura de mesagerie electronică, compatibile și interoperabile cu cele existente.

Totodată, soluția implementată va contribui la extinderea capabilităților de apărare cibernetică împotriva amenințărilor specifice serviciilor de poștă electronică, prin

utilizarea unor mecanisme avansate de filtrare, detecție și analiză comportamentală a amenințărilor informatice.

Sistemul de protecție pentru soluția de mesagerie electronică va asigura protecția avansată a fluxurilor de e-mail, analiza fișierelor și atașamentelor suspecte în medii izolate de tip sandbox, precum și identificarea și blocarea amenințărilor informatice avansate, inclusiv a atacurilor de tip Advanced Persistent Threat (APT).

Prin realizarea acestei achiziții se asigură creșterea nivelului de reziliență cibernetică a infrastructurii de mesagerie electronică a MAI, standardizarea configurațiilor de securitate, administrarea unitară a politicilor de protecție și menținerea disponibilității serviciilor IT critice, inclusiv în situații de incident major sau dezastru.

Soluția va permite replicarea în regim 1:1 atât a configurației infrastructurii (ce rulează în mod activ) de securitate, cât și a capabilităților de procesare a fluxurilor de e-mail între site-ul principal și site-ul DR/BC.

Soluția oferită trebuie să se integreze nativ cu infrastructura existentă din site-ul principal, care include echipamente dedicate de securitate pentru mesagerie electronică (email security gateway și sandbox), configurate în cluster redundant, asigurând sincronizarea politicilor de securitate, schimbul de informații privind amenințările și funcționarea unitară a mecanismelor de protecție.

Integrarea va fi descrisă detaliat în propunerea tehnică, ofertantul având obligația de a prezenta arhitectura de integrare, fluxurile de date și mecanismele de interoperabilitate cu sistemele existente.

2.5. Cadrul general al sectorului în care Autoritatea contractantă își desfășoară activitatea

Cadrul general, atribuțiile și funcțiile pe care le îndeplinește Autoritatea contractantă sunt detaliate în O.U.G. nr. 30 din 25 aprilie 2007 privind organizarea și funcționarea Ministerului Afacerilor Interne, cu modificările și completările ulterioare.

Direcția Generală pentru Comunicații și Tehnologia Informației este unitatea centrală de specialitate a Ministerului Afacerilor Interne care asigură organizarea, coordonarea și controlul activității ministerului în domeniul comunicațiilor și tehnologiei informației.

Activitatea Direcției se desfășoară în conformitate cu prevederile legilor, ordonanțelor și hotărârilor Guvernului României, ale ordinelor și instrucțiunilor Ministrului Afacerilor Interne, Agendei digitale a MAI (2023-2030), precum și cu planurile de cooperare și programele anuale de acțiuni și este destinată conducerii activității de comunicații și tehnologia informației în Ministerul Afacerilor Interne.

2.6. Factori interesați și rolul acestora

Structurile vizate direct sau indirect de rezultatele achiziției sunt structuri ale Aparatului Central al MAI, precum și unitățile subordonate ale Ministerului Afacerilor Interne.

3. PRODUSELE SOLICITATE

3.1 Obiectivul general la care contribuie furnizarea produselor

Obiectivul general al proiectului MAI Digital este reprezentat de transformarea MAI într-o entitate modernă și digitalizată care să furnizeze servicii publice electronice de înaltă calitate, disponibilitate și adaptate nevoilor cetățenilor și mediului de afaceri. Scopul principal al proiectului vizează accelerarea procesului de digitalizare a serviciilor publice furnizate de către structurile MAI, prin dezvoltarea de noi servicii publice electronice, precum și îmbunătățirea, creșterea gradului de sofisticare a serviciilor publice electronice, cu accent pe creșterea eficienței și calității interacțiunii dintre cetățeni, mediu de afaceri cu administrația publică.

Obiectivul general al achiziției îl reprezintă implementarea unui sistem de protecție pentru soluția de mesagerie electronică în site-ul Disaster Recovery și Business Continuity (DR/BC), bazat pe echipamente hardware dedicate de tip email gateway security și sandbox hardware licențiat, integrate cu infrastructura existentă din site-ul principal și aliniate din punct de vedere al subscripțiilor, în vederea asigurării unei protecții unitare, creșterii nivelului de securitate a fluxurilor de e-mail, consolidării rezilienței infrastructurii IT și asigurării continuității operaționale a serviciilor de mesagerie electronică în scenarii de avarie sau dezastru.

3.2 Obiectivele specifice la care contribuie furnizarea produselor și serviciilor

Achiziția va contribui la atingerea următoarelor obiective specifice:

- ✓ creșterea numărului de servicii electronice și a gradului de sofisticare a serviciilor publice electronice furnizate de către structurile MAI;
- ✓ creșterea eficienței administrative și reducerea birocrăției în cadrul MAI;
- ✓ minimizarea prezenței fizice a cetățenilor la sediile instituțiilor, generând economii semnificative în costuri și timp pentru cetățeni, mediul de afaceri și prin diminuarea cheltuielilor operaționale ale MAI;
- ✓ sporirea atractivității serviciilor publice electronice oferite de structurile MAI pentru cetățeni, prin reducerea disconfortului creat de deplasarea cetățenilor la ghișeu/poștă, îmbunătățirea calității, disponibilității și rezilienței serviciilor publice electronice furnizate de către structurile MAI.
- ✓ extinderea serviciilor de poștă electronică în site-ul Disaster Recovery și Business Continuity (DR/BC), prin implementarea soluțiilor dedicate de securitate pentru infrastructura de mesagerie electronică;

✓ îmbunătățirea nivelului de securitate al fluxurilor de e-mail, prin implementarea mecanismelor avansate de protecție împotriva spamului, malware-ului și altor amenințări informatice;

✓ creșterea capacității de detecție și analiză a amenințărilor informatice avansate, inclusiv a atacurilor de tip Advanced Persistent Threat (APT), prin utilizarea tehnologiilor de analiză comportamentală;

✓ asigurarea continuității operaționale a serviciilor de mesagerie electronică în scenarii de incident major sau dezastru, prin integrarea infrastructurii din site-ul DR/BC cu sistemele existente;

✓ creșterea rezilienței infrastructurii IT și a serviciilor publice electronice furnizate de MAI, prin consolidarea mecanismelor de securitate cibernetică pentru serviciile critice;

✓ asigurarea continuității operaționale prin integrarea infrastructurii din site-ul DR/BC cu infrastructura existentă, în vederea funcționării unitare a serviciilor de securitate.

3.3 Descrierea produselor solicitate

În derularea contractului, activitatea contractantului va fi condusă de următoarele principii:

i. Contractantul acționează în interesul autorității/entității contractante pe durata furnizării produselor, în condițiile și cu limitele descrise în documentația aferentă prezentei proceduri de atribuire;

ii. Contractantul acționează în sensul realizării obiectivelor prezentate pentru contract în ceea ce privește optimizarea folosirii resurselor necesare îndeplinirii obiectivelor contractului.

3.3.1. Produse solicitate

Nr. Crt.	Denumire produs	Cantitate	Unitate de măsură	Loc de livrare	Termen de livrare solicitat	Specificații tehnice SAU cerințe funcționale minime	Specificații tehnice SAU cerințe funcționale extinse	Durata minimă garanție/termen de valabilitate
----------	-----------------	-----------	-------------------	----------------	-----------------------------	---	--	---

1.	“Sistem de protecție pentru soluția de mesagerie electronică” pentru extindere a capacității de apărare cibernetică împotriva amenințărilor specifice serviciilor de poștă electronică în site-ul DR/BC	1	complet	locația Autorității contractante din București și/sau Brașov	30 de zile lucrătoare	Conform Anexei nr.1 la CS	Conform Anexei nr.1 la CS	Minim 36 de luni
----	---	---	---------	--	-----------------------	---------------------------	---------------------------	------------------

În cadrul prezentei achiziții, produsele și materialele încorporate ce urmează a fi achiziționate trebuie să fie noi, nefolosite, de asemenea, vor fi oferite cele mai recente modele. Produsele și materialele încorporate ce urmează a fi achiziționate ar trebui să încorporeze cele mai recente îmbunătățiri în proiectare și materiale.

Orice referire la standarde va fi însoțită de mențiunea “Sau echivalent”, fiind în sarcina ofertantului de a demonstra echivalența în cazul în care produsele furnizate sunt conforme cu un standard echivalent celui menționat în Caietul de sarcini.

Specificațiile tehnice din prezentul caiet de sarcini care precizează un anumit producător, o anumită origine sau un anumit procedeu care caracterizează produsele sau serviciile furnizate și care se referă la mărci, brevete, tipuri, la o origine sau la o producție specifică se consideră a fi însoțite de cuvintele “sau echivalent”, indiferent dacă aceste cuvinte sunt prevăzute expres sau nu în prezentul document.

3.3.2. Timp de funcționare (disponibilitate) a produsului

Contractantul va configura echipamentele și licențele livrate astfel încât să fie asigurată o disponibilitate ridicată a sistemului.

3.3.3 Do No Significant Harm (DNSH)

Prestatorul declară și garantează că produsele și serviciile furnizate în temeiul prezentului acord respectă principiile “Do No Significant Harm (DNSH)”, astfel cum sunt prevăzute de Regulamentul delegat (UE) 2021/2139, neaducând prejudicii semnificative obiectivelor de mediu.

3.3.4 Acces al autorităților naționale

Prestatorul se obligă să asigure accesul neîngrădit al autorităților naționale cu

atribuții de verificare, control și audit, al serviciilor Comisiei Europene, al Curții Europene de Conturi, al reprezentanților Direcției Naționale Anticorupție, al reprezentanților Parchetului European – EPPO, al reprezentanților serviciului specializat al Comisiei Europene - Oficiul European pentru Lupta Antifraudă - OLAF, precum și al reprezentanților Departamentului pentru Lupta Antifraudă - DLAF, în limitele competențelor ce le revin, în cazul în care aceștia efectuează investigații/verificări/controale/audituri la fața locului și solicită declarații, evidențe, documente justificative, informații și date statistice referitoare la investiție.

3.4. Extensibilitate/Modernizare

Nu este cazul.

3.5. Furnizarea de produse de generație superioară, dacă este cazul

Nu este cazul.

3.6. Garanție

Toate produsele trebuie să fie acoperite de garanție și subscripție pentru cel puțin perioada solicitată pentru fiecare produs, minim 36 luni din prezentul caiet de sarcini. Perioada de garanție începe de la data semnării procesului verbal de recepție cantitativă și calitativă fără obiecțiuni. Garanția va asigura înlocuirea oricărei componente defecte, costurile înlocuirii fiind suportate de către Contractant (piese, deplasare și manoperă).

În cazul în care producătorii oferă o perioadă de garanție mai mare decât perioada minimă indicată de Autoritatea contractantă, perioada ofertată pentru sistemul livrat va fi cel puțin cât perioada oferită de producător.

În perioada de garanție, Contractantul se obligă să asigure constatarea defecțiunilor hardware și remedierea defectelor. Remedierea defecțiunilor se constată de către MAI în locația unde este instalat echipamentul.

În situația în care este necesară transportarea echipamentului în afara locației în care acesta este instalat, toate mediile de stocare a datelor vor fi reținute de către MAI (hard-discurile vor fi scoase din echipament și păstrate la sediul MAI);

Transportul în siguranță al produsului predat de Autoritatea contractantă intră în responsabilitatea contractantului și va fi efectuat fără costuri suplimentare.

La finalizarea fiecărei intervenții în cadrul perioadei de garanție se va întocmi o fișă de intervenție care va conține următoarele detalii: data intervenției, descrierea intervenției, modalitatea de rezolvare a intervenției (reparație/înlocuire), durata de intervenție și confirmarea intervenției prin semnăturile reprezentanților Contractantului și MAI;

În cazul în care durata de remediere a defecțiunii unui echipament depășește 2 zile lucrătoare, Contractantul va furniza un echipament înlocuitor similar, din punct de vedere al funcționalității și al specificațiilor tehnice, pentru a asigura continuitatea serviciilor informatice până la remedierea defecțiunii. Repunerea în funcțiune nu trebuie să depășească 5 zile lucrătoare.

În cazul defectării totale a echipamentului, ori în cazul imposibilității depanării din motive neimputabile Contractantului, acesta se obligă să îl înlocuiască cu unul nou cu caracteristici tehnice similare sau superioare, care va rămâne în proprietatea Autorității Contractante. Înlocuirea echipamentului se va efectua pe cheltuiala exclusivă a Contractantului, în ziua imediat următoare expirării celor 5 zile lucrătoare menționate mai sus. Contractantul are obligația să prezinte documente justificative pentru motivarea imposibilității depanării. Perioada de garanție va fi extinsă cu o perioadă de timp egală cu durata de indisponibilizare a echipamentului.

Indiferent de defectul produsului oferat, ce necesită, dacă este cazul, a fi înlocuit în perioada de garanție, mediile de stocare de date de tip HDD, SSD, USB stick-uri, tape, defecte sau nu sau orice alt mediu amovibil, nu se vor returna Contractantului, acestea urmând să rămână în posesia autorității contractante. În cazul echipamentelor care nu permit detașarea mediilor de stocare, înainte de preluarea echipamentelor defecte în service, contractantul trebuie să șteargă datele de pe mediile de stocare utilizând un produs software care se regăsește în CATALOGUL NAȚIONAL CU PACHETE, PRODUSE ȘI PROFILE DE PROTECȚIE INFOSEC – ultima versiune. Activitatea de ștergere iremediabilă a datelor de pe mediile de stocare se va face la sediul autorității contractante în prezența reprezentanților acesteia, rezultând un document prin care să fie dovedită această activitate. În situația în care pe echipamentele defecte nu se poate utiliza produsul software pentru ștergerea iremediabilă a datelor de pe mediile de stocare, acestea vor rămâne în proprietatea autorității contractante, iar contractantul se obligă să livreze un echipament nou cu caracteristici tehnice similare sau superioare.

Garanția va fi de minim 36 luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar fără costuri suplimentare.

3.7 Livrare, ambalare, etichetare, transport și asigurare pe durata transportului

Produsele vor fi livrate la locul indicat în contract în intervalul orar 08:00 – 16:00, la sediile autorității contractante din București și/sau Brașov. Fiecare produs va fi însoțit de toate subansamblele/părțile componente necesare punerii și menținerii în funcțiune.

Termenul de livrare, instalare, punere în funcțiune, testare și transfer de cunoștințe este de 30 de zile lucrătoare.

Produsele se consideră livrate când toate activitățile referitoare la livrare în cadrul contractului au fost realizate, produsul funcționează la parametrii agreeți și este acceptat de Autoritatea contractantă. Produsele vor purta marcajele originale ale producătorului.

Produsele livrate trebuie să fie însoțite obligatoriu de următoarele documente, după caz:

- a) aviz de însoțire a mărfii;
- b) certificate / declarații de calitate și certificate de conformitate emise de un organism acreditat, în conformitate cu legislația aplicabilă sau declarații de conformitate

emise de producător, pentru fiecare produs livrat;

c) CD/DVD/USB-urile suport de la producător (dacă acestea sunt disponibile) sau să se indice în documentație de unde se pot descărca de la producător;

d) document/documente în format digital cu liste ce conțin Serial-Number pentru fiecare produs/componentă livrată;

e) certificate de garanție pe perioada ofertată, minim 36 luni, emise de producător sau Contractant.

În vederea asigurării corespondenței, justificării și trasabilității între reperatele menționate în caietul de sarcini și cele oferite, denumirea echipamentelor/licențelor din factură, aviz de însoțire a mărfii și din certificatul de garanție va fi aceeași cu cea din oferta tehnică/financiară a contractantului.

Contractantul va preciza pe toate documentele de însoțire a echipamentelor/licențelor livrate contractul în baza căruia s-a făcut livrarea.

Contractantul va ambala și eticheta echipamentele furnizate astfel încât să prevină orice daună sau deteriorare în timpul transportului acestora către destinația stabilită. Dacă este cazul, ambalajul trebuie prevăzut astfel încât să reziste, fără limitare, manipulării accidentale, expunerii la temperaturi extreme, precipitațiilor din timpul transportului și depozitării în locuri deschise.

Contractantul trebuie să instaleze toate produsele în mod corespunzător, asigurându-se în același timp că spațiile unde s-a realizat instalarea rămân curate. După livrarea și instalarea produselor, Contractantul va elimina toate deșeurile rezultate și va lua toate măsurile adecvate pentru a aduna toate ambalajele și pentru eliminarea acestora de la locul de instalare.

Contractantul va asigura transportul și descărcarea produselor până la locul de livrare indicat de Autoritatea contractantă. Predarea produselor către reprezentanții Autorității Contractante se va face de luni până vineri în intervalul orar 08:00 – 16:00.

Contractantul este responsabil pentru livrarea în termenul agreat a produselor și se consideră că a luat în considerare toate dificultățile pe care le-ar putea întâmpina în acest sens și nu va invoca niciun motiv de întârziere sau costuri suplimentare.

Furnizorul trebuie să ia toate măsurile necesare asigurării vizibilității fondurilor finanțate de Uniunea Europeană. Aceste măsuri trebuie să fie în acord cu regulile de implementare a proiectelor finanțate din Programul Creștere Inteligentă, Digitalizare și Instrumente Financiare 2021-2027 (PCIDIF).

Pentru asigurarea vizibilității acțiunii de finanțare a contractului de furnizare, pe produse se va aplica pe partea cea mai vizibilă pentru public un autocolant care să conțină elemente informative obligatorii, conform cerințelor din Ghidul de Identitate Vizuală - Vizibilitate, Transparență și Comunicare în Perioada de Programare 2021-2027.

3.8. Operațiuni cu titlu accesoriu

3.8.1. Instalare, punere în funcțiune, transfer de cunoștințe, testare

Produsele vor fi livrate, instalate, configurate și testate în locațiile Autorității Contractante menționate în contract.

Contractantul trebuie să realizeze următoarele activități:

- Transportul, instalarea, configurarea echipamentelor conform cerințelor din prezentul caiet de sarcini;
- Livrarea documentației tehnice (documentație de instalare și configurare);
- Integrarea soluției livrate cu infrastructura existentă din site-ul principal, inclusiv configurarea mecanismelor de sincronizare a politicilor de securitate, schimbului de indicatori de compromitere și a fluxurilor de analiză a amenințărilor, **fără a impacta condițiile de garanție și suport ale soluțiilor/echipamentelor existente.**
- Testarea produsului furnizat pe baza documentației elaborate de Contractant și agreeată de reprezentanții Autorității Contractante;
- Transfer de cunoștințe către minim 4 specialiști din cadrul personalului Autorității Contractante pentru utilizarea echipamentelor care fac obiectul contractului;
- Toate cablurile necesare pentru alimentare, interconectare, cât și alte accesorii sau conectori pentru funcționarea soluției/echipamentului vor fi puse la dispoziție de către Contractant.

Ofertantul va descrie în propunerea tehnică etapele, metodele și resursele utilizate pentru realizarea integrării, precum și eventualele condiții sau dependențe tehnice.

Integrarea va fi validată în cadrul procesului de testare și recepție, prin verificarea funcționării unitare a soluției cu infrastructura existentă.

În vederea pregătirii instalării, după semnarea contractului, Contractantul va realiza inspecția sediului Autorității Contractante și se va documenta cu privire la modalitatea de instalare.

Pentru a asigura funcționarea produselor la parametri agreeți, Contractantul va efectua testarea pe cheltuiala sa și fără nici un fel de costuri din partea Autorității Contractante. Contractantul rămâne responsabil pentru protejarea echipamentelor luând toate măsurile adecvate pentru a preveni lovituri, zgârieturi și alte deteriorări, până la recepția finală de către Autoritatea contractantă.

Toate echipamentele și licențele vor fi noi și nefolosite. Nu se acceptă produse remanufacturate sau restaurate și/sau care au în componență elemente/componente care au fost folosite anterior. La livrare, echipamentele și licențele nu trebuie să aibă anunțat sfârșitul perioadei de vânzare sau de suport (End of Sales, End of Support).

3.8.2. Instruirea personalului pentru utilizare

Contractantul este responsabil pentru instruirea la fața locului a personalului desemnat de Autoritatea contractantă. Scopul instruirii este de a transfera cunoștințele necesare pentru operarea, administrarea și configurarea echipamentelor de securitate furnizate, respectiv a soluțiilor dedicate protecției serviciilor de poștă electronică, astfel încât personalul Autorității Contractante să poată utiliza și gestiona în mod eficient

funcționalitățile acestora. Numărul persoanelor care vor fi instruite este de minim 4 specialiști. Durata sesiunii de instruire va fi de minim 2 zile lucrătoare, sesiunea se va desfășura în limba română.

Instruirea va fi organizată după ce produsele sunt funcționale și va avea ca scop transferul de cunoștințe necesare operării și administrării sistemului furnizat. Conținutul detaliat al sesiunii de instruire și obiectivele ce trebuie parcurse sunt prevăzute în cadrul specificațiilor tehnice din Anexa nr. 1 la prezentul Caiet de sarcini, secțiunea referitoare la transferul de cunoștințe. Contractantul trebuie să propună orice subiect suplimentar care ar putea fi necesar pentru a se asigura că personalul autorității contractante este pe deplin instruit pentru a asigura utilizarea corespunzătoare a produselor.

3.9. Servicii de mentenanță

3.9.1. Mentenanța corectivă în perioada de garanție

Nu este cazul.

3.9.2. Mentenanța preventivă în perioada de garanție

Nu este cazul.

3.9.3. Mentenanța evolutivă în perioada de garanție

Nu este cazul.

3.10. Suport tehnic

Contractantul va avea acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate, precum și accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software oferite (firmware, drivere componente, pachete software de la producător incluse în echipamentul oferit), fără costuri suplimentare.

Suportul va include:

- acces la actualizări publicate de producător;
- acces la biblioteca de cunoștințe (knowledge base) a producătorilor;
- posibilitatea de comunicare a cererilor de asistență tehnică direct către punctul unic de contact pentru serviciile de garanție și suport tehnic al Contractantului;
- majorarea perioadei de garanție cu timpul de nefuncționare a produselor software instalate, respectiv soluțiilor software configurate;
- remedierea oricărei neconcordanțe a produselor (soluțiilor) software față de cerințele enunțate în Caietul de sarcini;
- Contractantul va furniza/informa pe toată durata garanției produsului toate update-urile care duc la fixarea unor probleme sau facilități de care utilizatorul are nevoie. Operațiunea de update se face de comun acord cu Autoritatea contractantă, fără a afecta stabilitatea/funcționalitatea soluției;

- serviciile de instalare și configurare a componentelor vor fi asigurate de Contractant prin personal certificat/autorizat;

- alte cerințe formulate expres în Caietul de sarcini și anexele la acesta.

Ofertantul va furniza servicii de suport tehnic pe perioada garanției, care vor cuprinde:

- Suport pentru produsele furnizate, utilizate în baza Service Level Agreement(SLA);

- Marcarea finalizării cererii și comunicarea modalității de soluționare completă și definitivă a cererii către Autoritatea contractantă.

Pentru operativitate va fi desemnat un singur punct de intrare pentru toate incidentele semnalate de Autoritatea contractantă și Contractantul va răspunde în timp util la orice incident în funcție de nivelul acestuia. Solicitățile primite de la Autoritate contractantă vor fi transmise prin e-mail/telefon/aplicație de ticketing.

Contractantul va răspunde în timp util la orice incident semnalat de Autoritatea contractantă, în funcție de nivelul incidentului. Fiecare incident este caracterizat de un nivel de prioritate (definit în tabelul de mai jos), care va evidenția impactul acestuia asupra funcționalităților produsului.

Nivelul de prioritate poate fi modificat, cu acordul părților, în funcție de evoluția incidentului.

Serviciile de Suport tehnic vor fi furnizate sub incidența Clauzelor de confidențialitate.

Contractantul va trebui să respecte următorii timpi de răspuns:

Nivel prioritate	Timp de răspuns	Timp de implementare soluție provizorie	Timp de rezolvare	Orar de funcționare
Urgent	30 min	12 ore	1 zi lucrătoare	24x7
Critic	4 ore	1 zi lucrătoare	2 zile lucrătoare	24x7
Major	8 ore	2 zile lucrătoare	4 zile lucrătoare	24x7
Minor	12 ore	2 zile lucrătoare	5 zile lucrătoare	8x5

Nerespectarea timpilor de mai sus dă dreptul Autorității contractante de a solicita penalități / daune interese în conformitate cu clauzele contractului de achiziție publică/ sectorială de produse.

În cazul incidentelor cu nivel de prioritate "urgent", "critic" și "major" asistența va fi asigurată 24x7, fiind disponibilă până când problema va fi rezolvată. Pentru aceasta, Autoritatea contractantă va furniza o persoană de contact, disponibilă 24x7, care să furnizeze informații, să testeze soluții și să aplice soluțiile furnizate.

Definiții aplicabile:

Urgent - incidentul are impact major asupra funcționării echipamentelor. Problema împiedică desfășurarea activității Autorității Contractante, procesul de activitate este serios afectat și nu mai poate continua.

Critic - impact semnificativ asupra funcționării echipamentelor. Problema împiedică desfășurarea în condiții normale a activității Autorității Contractante. Nici o soluție alternativă nu este disponibilă, însă activitatea Autorității Contractante poate totuși continua, însă într-un mod restrictiv.

Major - impact mediu asupra desfășurării activității Autorității contractante. Problema afectează minor funcționalitățile produsului. Impactul reprezintă un inconvenient care necesită soluții alternative pentru refacerea funcționalităților.

Minor - impact minim asupra desfășurării activității Autorității contractante. Problema nu afectează funcționalitățile produsului. Rezultatul este o eroare minoră care nu împiedică desfășurarea în bune condiții a activității Autorității contractante.

Timp de Răspuns: Intervalul de timp scurs de la semnalarea incidentului de către Autoritatea contractantă și răspunsul primit de la Contractant.

Timp de implementare soluție provizorie: Intervalul de timp scurs de la semnalarea incidentului de către Autoritatea contractantă și adoptarea unei soluții provizorii, temporare, care să permită funcționarea produsului/produselor fără afectarea funcționalităților critice, până la rezolvarea definitivă a incidentului, cu asigurarea integralității funcționale și a performanței echipamentului.

Timp de Rezolvare: Intervalul de timp scurs de la semnalarea incidentului de către Autoritatea contractantă până la rezolvarea finală a incidentului.

Furnizorul va asigura în această perioadă de garanție:

- Suport telefonic de luni până vineri orele 8.00 – 16.00;
- Suport în locație sau la distanță;

Produsele livrate nu trebuie să fie end-of-life/end-of-sale/end-of-support. În cazul în care, în perioada desfășurării achiziției, produsul devine end-of-life/end-of-sale/end-of-support, acesta trebuie să fie înlocuit cu un produs care să asigure minim cerințele caietului de sarcini.

Contractantul are obligația de a remedia incidentele constatate de Autoritatea contractantă în perioada de garanție, iar termenul de garanție se va prelungi cu durata necesară soluționării problemelor sau incidentelor identificate.

3.11. Piese de schimb și materiale consumabile pentru activitățile din programul de mentenanță corectivă după expirarea garanției

Nu este cazul.

3.12. Mediul în care este operat produsul

Nu este cazul.

3.13. Constrângeri privind locația unde se va efectua livrarea/instalarea

Accesul personalului Contractantului în locația unde se va efectua livrarea/instalarea/configurarea se va face prin transmiterea către Autoritatea contractantă a listei cu persoanele autorizate de către Contractant pentru prestarea

serviciilor. De asemenea, persoanele autorizate de către Contractant vor trebui să aibă asupra lor documentul de identitate la momentul accesului în locație.

4. ATRIBUȚIILE ȘI RESPONSABILITĂȚILE PĂRȚILOR

În raport cu produsele solicitate și cu cerințele stipulate în prezentul Caiet de Sarcini, responsabilitățile și atribuțiile părților sunt:

4.1 Atribuțiile și responsabilitățile Contractantului

✓ mobilizarea de resurse suficiente și cu expertiză adecvată pentru a asigura gestionarea contractului, astfel cum este solicitat la nivelul Caietului de Sarcini

✓ livrarea produselor, îndeplinirea obligațiilor contractuale, cu respectarea bunelor practici din domeniu, a prevederilor legale și contractuale relevante, astfel încât să se asigure că obligațiile sunt îndeplinite la parametrii solicitați

✓ activarea subscripțiilor necesare pentru funcționarea componentelor livrate.

✓ asigurarea unui grad de flexibilitate în planificarea modalității de gestionare a contractului, pe toată durata de derulare a contractului

✓ transmiterea datelor de identificare și de contact ale personalului alocat pentru executarea contractului

✓ colaborarea cu personalul autorității/entității contractante alocat pentru verificarea produselor livrate și realizarea recepțiilor, asigurarea instrumentelor de testare

✓ reducerea, în măsura posibilă, la minim, a situațiilor de întârzieri în efectuarea livrărilor, minimizând astfel impactul negativ asupra activității autorității/entității contractante

✓ asigurarea că orice documente, documentații și/sau instrucțiuni furnizate către personalul autorității/entității contractante sunt exacte și elaborate în conformitate cu bunele practici specifice în domeniu

✓ colaborarea cu personalul autorității/entității contractante alocat pentru furnizarea produselor care fac obiectul contractului și pentru asigurarea serviciilor accesorii

✓ transferul de cunoștințe către personalul Autorității contractante pentru utilizarea produselor livrate

✓ asigurarea garanției și suportului tehnic al produselor livrate

✓ asigurarea disponibilității informațiilor și documentelor referitoare la contract / acordul-cadru cu ocazia misiunilor de control desfășurate de AMPoCIDIF/OIPoCIDIF sau de alte structuri cu competențe în controlul și recuperarea debitelor aferente fondurilor europene și/sau fondurilor publice naționale aferente acestora, după caz.

Obligațiile principale ale Ofertantului devenit Contractant se completează cu obligațiile prevăzute în condițiile contractuale.

4.2 Atribuțiile și responsabilitățile Autorității Contractante

- ✓ desemnarea unei persoane sau a unei echipe pentru monitorizarea contractului
- ✓ punerea la dispoziția Contractantului a tuturor informațiilor disponibile și necesare pentru derularea contractului în timpul stabilit și la nivelul de calitate și performanță prevăzut în Caietul de Sarcini
- ✓ asigurarea accesului în spațiile în care urmează a se realiza livrarea, după caz instalarea produselor
- ✓ mobilizarea tuturor resurselor care sunt în sarcina sa, pentru buna derulare a contractului
- ✓ colaborarea cu Contractantul pentru a identifica în timp util orice eventuale probleme care ar putea apărea pe parcursul derulării contractului
- ✓ asigurarea acurateții oricăror informații puse la dispoziția Contractantului pe durata derulării contractului
- ✓ monitorizarea îndeplinirii tuturor cerințelor din Caietul de Sarcini și a oricăror elemente ale Propunerii Tehnice și Financiare pe durata derulării contractului, efectuarea și păstrarea unei arhive cu înregistrări pentru documentarea nivelului de performanță a Contractantului
- ✓ notificarea Contractantului prin canalele de comunicație puse la dispoziție de acesta privind orice incidente sau disfuncționalități care intervin pe perioada de derulare a contractului
- ✓ verificarea tuturor documentelor asociate recepției produselor și serviciilor suport care fac obiectul contractului, respectiv care confirmă furnizarea produselor potrivit condițiilor de calitate stabilite în Caietul de sarcini

4.3. Alte atribuții și responsabilități

Contractantul are obligația de a începe executarea contractului după semnarea acestuia de către ambele părți și constituirea garanției de bună execuție.

Furnizarea produselor și serviciilor aferente în baza contractului trebuie finalizată în termenul convenit de părți, termen care se calculează de la data intrării în vigoare a contractului.

În cazul în care intervin motive de întârziere care nu se datorează Contractantului, sau apar alte circumstanțe neobișnuite susceptibile de a surveni, altfel decât prin încălcarea contractului de către Contractant, care îndreptățește Contractantul de a solicita prelungirea perioadei de furnizare a produselor sau a oricărei faze de instalare, punere în funcțiune, testare și transfer de cunoștințe, atunci părțile vor revizui, de comun acord, termenul de livrare și vor semna un act adițional.

Chiar dacă Autoritatea contractantă este de acord cu o prelungire a termenului de livrare, orice întârziere în îndeplinirea contractului din vina Contractantului dă dreptul Autorității contractante de a solicita penalități.

Contractantul are obligația de a înlocui bunurile oferite cu altele similare/superioare în cazul în care acestea sau anumite componente nu se mai fabrică

sau a fost interzisă comercializarea lor, prin legislația adoptată la nivelul Uniunii Europene, legislația națională, prin acorduri colective sau prin tratatele și acordurile internaționale, în acest sens urmând a se încheia act adițional.

5. DOCUMENTAȚII CE TREBUIE FURNIZATE AUTORITĂȚII CONTRACTANTE ÎN LEGĂTURĂ CU PRODUSUL

În cadrul recepției cantitative și calitative a produselor, furnizorul va prezenta integral documentațiile (specificații, certificate, etc.) tehnice aferente acestora, astfel cum au fost solicitate în prezentul caiet de sarcini.

De asemenea, Contractantul va elabora și preda către Autoritatea contractantă actualizări ale manualelor și documentațiilor destinate administratorilor ori de câte ori va fi necesar, pe perioada de garanție.

6. RECEPȚIA PRODUSELOR

Recepția va consta în verificarea cantitativă și calitativă a produselor livrate și se va efectua de către Autoritatea contractantă la destinația finală, cu sprijinul personalului Contractantului, într-un interval de maxim 15 zile lucrătoare de la furnizarea, instalarea, punerea în funcțiune, testarea produselor și transferul de cunoștințe și va fi finalizată prin încheierea proceselor-verbale de recepție semnate de reprezentanții Autorității Contractante și ai contractantului, după caz. Procesele-verbale de recepție calitativă și cantitativă vor include unul din următoarele rezultate:

- ✓ admiterea recepției
- ✓ respingerea recepției

Recepția cantitativă și calitativă a produselor se va face de către o comisie formată din reprezentanți ai Autorității contractante, la destinația finală prevăzută în contract.

Dacă unul din produse nu corespunde specificațiilor din oferta tehnică, Autoritatea contractantă are dreptul să îl respingă, iar Contractantul, fără a modifica prețul contractului, are una din obligațiile următoare:

- a. să înlocuiască produsele refuzate
- b. să facă toate modificările necesare pentru ca produsele să corespundă specificațiilor tehnice.

Nu se admit neconcordanțe între produsele livrate și specificațiile tehnice din caietul de sarcini și propunerea tehnică.

Constatarea de deficiențe în funcționarea produselor livrate sau neconcordanțe între caracteristicile tehnice și funcționale ofertate și produsele livrate, în timpul recepției, atrage după sine înlocuirea produselor, fără costuri suplimentare, cu produsele corespunzătoare, conform ofertei tehnice. Produsele livrate la care s-au constatat

neconformități, deficiențe sau lipsuri, vor fi consemnate într-un proces-verbal de recepție și vor fi înlocuite de către Contractant, fără costuri suplimentare, în termen de maxim 10 zile lucrătoare de la data constatării acestora.

După soluționarea eventualelor neconformități se va încheia procesul-verbal final de recepție cantitativă și calitativă, în termenul prevăzut la paragraful 1 al acestui capitol, semnat de reprezentanții Contractantului și ai Autorității contractante.

Factura va fi emisă, conform prevederilor legale în vigoare, numai după ce produsele au fost acceptate la recepție, prin semnarea, fără obiecțiuni, a Procesului verbal de recepție cantitativă și calitativă.

În cadrul recepției cantitative și calitative a produselor furnizate, Contractantul va prezenta integral documentațiile (specificații, certificate etc.) tehnice aferente acestora astfel cum au fost solicitate în prezentul caiet de sarcini.

Dreptul Autorității contractante de a inspecta, testa și, dacă este necesar, de a respinge produsele, nu va fi limitat sau amânat din cauza faptului că produsele au fost inspectate și testate de Contractant, cu sau fără participarea unui reprezentant al Achizitorului, anterior livrării acestora la destinația finală.

Recepția produselor este considerată finalizată după parcurgerea cu succes a testelor și semnarea, fără obiecțiuni, a Procesului verbal de recepție cantitativă și calitativă.

7. MODALITĂȚI ȘI CONDIȚII DE PLATĂ

Procesele-verbale de recepție cantitativă și calitativă, prin care produsele livrate/serviciile prestate sunt admise la recepție de către Autoritatea contractantă, vor însoți factura și reprezintă elementul necesar realizării plății, împreună cu celelalte documente justificative menționate la capitolul *Livrare*.

Contractantul va emite factura pentru produsele livrate, prin transmiterea acesteia, în mod gratuit, în format electronic, prin Sistemul național privind factura electronică RO e-Factura în situația în care furnizorul a optat pentru utilizarea Sistemului național privind factura electronică RO e-Factura, conform prevederilor Ordonanței de urgență nr. 120/2021, cu modificările și completările ulterioare. În cazul în care furnizorul nu este înscris în Sistemul național privind factura electronică RO e-Factura, factura se va transmite prin e-mail la adresa menționată în contract.

Factura va avea menționat numărul contractului, datele de emiterie și de scadență.

Odată cu emiterea facturii contractantul va transmite Autorității Contractante documentele justificative prevăzute mai jos, după caz:

- a) avizul de expediție a produselor;
- b) certificat de garanție emis de producător sau Contractant;
- c) Certificate de calitate și certificate de conformitate eliberate de producător în original sau în copie conformă cu originalul pentru fiecare produs livrat;
- d) CD/DVD-urile suport de la producător (dacă acestea sunt disponibile) sau să se indice în documentație unde se pot descărca de la producător;

e) documentație tehnică pentru fiecare tip de produs livrat;

f) document/documente în format digital cu liste ce conțin Serial-Number pentru fiecare produs/componentă livrată.

Factura va fi emisă după semnarea de către Autoritatea contractantă a procesului verbal de recepție calitativă și cantitativă, acceptat, după livrare, instalare și punere în funcțiune a produselor.

Plata se va realiza în termen de 30 de zile de la data recepției cantitativă și calitativă, fără obiecțiuni, a bunurilor furnizate / serviciilor prestate și emiterea facturii de către Contractant, conform prevederilor Legii nr. 72/2013 cu modificările și completările ulterioare.

8. CADRUL LEGAL CARE GUVERNEAZĂ RELAȚIA DINTRE AUTORITATEA CONTRACTANTĂ ȘI CONTRACTANT

În cazul în care intervin schimbări legislative, Contractantul 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.

Ofertantul devenit Contractant 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 enumerate în anexa X la Directiva 2014/24.

Actele normative și standardele indicate mai jos sunt considerate indicative și nelimitative; enumerarea actelor normative din acest capitol este oferită ca referință și nu trebuie considerată limitativă:

i. *Legea nr. 98/2016 privind achizițiile publice, cu modificările și completările ulterioare;*

ii. *HG nr. 395/2016 privind aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică/acordurilor cadru din Legea nr. 98/2016 privind achizițiile publice;*

iii. *Codul fiscal;*

iv. *Legea nr. 72/2013 privind măsurile pentru combaterea întârzierii în executarea obligațiilor de plată a unor sume de bani rezultând din contracte încheiate între profesioniști și între aceștia și autorități contractante.*

Instituțiile competente de la care furnizorii, executanții sau prestatorii pot obține informații privind reglementările obligatorii referitoare la protecția muncii, la prevenirea și stingerea incendiilor și la protecția mediului, care trebuie respectate pe parcursul îndeplinirii contractului și care sunt în vigoare la nivel național sunt:

✓ *Inspekția Muncii din subordinea Ministerului Muncii, Familiei, Tineretului și Solidarității Sociale; reglementările obligatorii referitoare la securitatea și sănătatea în*

muncă pot fi consultate pe pagina de Internet <https://www.inspectiamuncii.ro/-/legislatie-s-1>.

✓ Inspectoratul General pentru Situații de Urgență din subordinea Ministerului Afacerilor Interne; reglementările obligatorii referitoare la prevenirea și stingerea incendiilor pot fi consultate pe pagina de Internet <https://igsu.ro/>.

✓ Ministerul Mediului, Apelor și Pădurilor; Reglementările obligatorii referitoare la protecția mediului, pot fi consultate pe pagina de Internet <https://mmediu.ro/despre-noi/legislatie/>.

9. MANAGEMENTUL/GESTIONAREA CONTRACTULUI ȘI ACTIVITĂȚILE DE RAPORTARE ÎN CADRUL CONTRACTULUI

Autoritatea contractantă: Ministerul Afacerilor Interne prin Direcția Generală pentru Comunicații și Tehnologia Informației (DGCTI).

Fiecare parte contractantă are obligația coordonării propriilor resurse și a activităților pentru derularea contractului, în conformitate cu atribuțiile precizate în caietul de sarcini.

Autoritatea contractantă și Contractantul identifică acțiunile corective pentru abordarea abaterilor constatate față de prevederile contractului.

Pe parcursul derulării contractului, Autoritatea contractantă verifică dacă toate activitățile planificate au fost realizate conform clauzelor contractuale, produsele/operațiunile accesorii contractate au fost livrate/prestate și admise la recepție în cantitățile contractate și cu respectarea cerințelor caietului de sarcini. Autoritatea contractantă se asigură pe toată perioada derulării contractului și nu doar la finalizarea/terminarea acestuia că activitățile planificate au fost realizate, cerințele stabilite au fost îndeplinite, serviciile au fost prestate, tehnica de calcul furnizată.

Contractantul este responsabil în totalitate de asigurarea managementului contractului din punct de vedere administrativ și financiar, sens în care va fi orientat spre obținerea rezultatelor stabilite pentru îndeplinirea obiectivelor. Acesta trebuie să respecte condițiile formulate în contract.

10. EVALUAREA PERFORMANȚEI CONTRACTULUI

Nu este cazul

11. ANEXĂ

Anexa nr. 1 - Specificații tehnice

Anexa nr. 2 - Factori de evaluare și punctaj

Specificații tehnice minime

Componenta 1 – „Sistem de protecție pentru soluția de mesagerie electronică” în site-ul Disaster Recovery și Business Continuity (DR/BC), destinat extinderii capacității de apărare cibernetică împotriva amenințărilor specifice serviciilor de poștă electronică, bazat pe soluții tip appliance destinat detectării programelor malware și a atacurilor de tip APT (Advanced Persistent Threats) cu subscripție și suport pe o perioadă de minim 36 luni

1. Caracteristicile tehnice generale:

- Capacitate de inspecție a fișierelor prin sandboxing: minim 160.000 de fișiere unice/oră;
- Capacitate de Throughput: minim 4 Gbps;
- Număr de mașini virtuale utilizate pentru inspecție: minim 8 instalate și licențiate cu posibilitate de extindere până la un număr de minim 56;
- Să suporte corelarea cu tehnicile din platforma MITRE ATT&CK;
- Montare în rack: DA;
- Surse redundante de putere;
- Interfețe echipate cu module SFP+: minim 8 x 10GB, tip conector LC duplex;
- Spațiu de stocare: minim 4 x 2 TB , hot swappable;
- Condiții de alimentare: 100 - 240 V, 50—60 Hz;
- Număr de surse de alimentare: 2
- Se vor asigura toate accesoriile / licențele / kit-urile gratuit, necesare punerii în funcțiune și integrării în subsistemul actual de securitate pentru mesagerie electronică, chiar dacă acestea nu au fost solicitate în mod expres în prezentul caiet de sarcini.

1. Funcționalități generale:

- a) Administrare/configurare prin WEB UI (HTTP/HTTPS), secure command shell (SSH), command line interface (CLI);
- b) Alertare personalizabile/detaliată, prin e-mail, în cazul detectării unui atac/program malware;
- c) Vizualizare informații sistem/resurse;
- d) Vizualizare stare licențe;
- e) Vizualizare statistică privind numărul de fișiere inspectate;

- f) Vizualizare statistică privind atacurile/programele malware detectate;
- g) Vizualizare statistică privind fișierele suspecte clasificate în funcție de gradul de risc;
- h) Vizualizare statistici de activitate în funcție de gravitatea atacurilor/programele malware detectate;
- i) Funcționalitate de export/import a configurației;
- j) Opțiune de încărcare a configurației din fabrică;
- k) Opțiune pentru actualizarea automată a mașinilor virtuale;
- l) Funcționalitatea hardware trebuie să fie appliance cu OS;
- m) Actualizare automată a semnăturilor de securitate;
- n) Logare privind activitatea sistemului.

2. Funcționalități de detecție a fișierelor malware și a atacurilor:

- a) Posibilitate de instalare în rețea în mod de operare sniffer (analiza traficului capturat) pentru analiza fișierelor transferate prin protocoalele HTTP, FTP, POP3, IMAP, SMTP, SMB;
- b) Să fie integrat cu o bază de date antivirus;
- c) Posibilitate de integrare cu o soluție destinată protecției antispam a traficului email cu posibilitatea scanării traficului SMTP, POP3, IMAP;
- d) Posibilitate de încărcare manuală a fișierelor în scopul inspecției acestora;
- e) Detectarea programelor malware pe baza de semnături antivirus;
- f) Detectarea atacurilor APT sau a programelor malware prin analiza comportamentală (sandboxing);
- g) Subsistemul trebuie să poată analiza comportamentul programelor inspectate prin execuția acestora în cadrul unor sisteme de operare virtualizate minim de tip Windows (10, 11), Linux și macOS;
- h) Subsistemul trebuie să permită personalizarea imaginilor VM;
- i) Subsistemul trebuie să permită analiza următoarelor tipuri de fișiere: arhive, executabile, PDF, MS Office, script files, Flash, Java etc.
- j) Subsistemul trebuie să permită analiza fișierelor fără a impune o limită de mărime a acestora;
- k) Subsistemul trebuie să poată analiza modificările induse de execuția programelor în cadrul sistemelor de operare virtualizate (regiștri, apeluri de sistem, procese pornite);
- l) Subsistemul trebuie să poată analiza conexiunile inițializate de programele inspectate în cadrul sistemelor de operare virtualizate (URL-uri accesate, rețele de tip Botnet);
- m) Subsistemul trebuie să genereze rapoarte privind activitatea programelor inspectate în cadrul sistemelor de operare virtualizate (screenshot-uri, trafic de rețea, listă cu calea fișierelor accesate și modificate);
- n) Posibilitate de a trimite automat fișierele suspecte pentru analiza mai detaliată a acestora, efectuată de producător;

- o) Suport pentru reguli Yara;
- p) Să detecteze și să protejeze împotriva atacurilor de tip malware zero-day;
- q) Să identifice în timp real site-urile de „Phishing” zero-day sau echivalent;
- r) Licențe pentru mașinile virtuale (exemplu: Windows, Office, Mac).

3. Garanție și suport

- a) Garanție echipamente de securitate minim 36 luni;
- b) Subscripția și suportul vor fi de tip Enterprise cu pachet ATP (Advanced Threat Protection) sau echivalent, pentru o perioadă de minim 36 luni.

4. Condiții migrare configurație echipamente existente

Se va asigura configurarea în clusterul existent de echipamente tip Sanbox de la nivelul Beneficiarului, astfel încât impactul asupra funcționalităților și sistemelor în producție să fie unul minim, **fără a impacta condițiile de garanție și suport ale soluțiilor/echipamentelor existente.**

Clusterul existent la nivelul Beneficiarului include următoarele echipamente FortiSandbox 3000G.

Se vor asigura script-uri cu titlu gratuit dacă acestea sunt necesare pentru punerea în funcțiune și operaționalizarea soluției.

5. Transferul de cunoștințe

1. Configurare de bază:

-instalare inițială și configurare de bază a echipamentului, incluzând setările rețelei, integrările esențiale și configurarea accesului la interfața de administrare. Cerințe hardware: montare rack, surse de alimentare redundante, conexiuni.

2. Configurare fizică: conectarea cablurilor și surselor de alimentare.

3. Configurare inițială software:

- Web UI, CLI, etc.
- Setarea IP-urilor, conectarea la rețea, și integrarea cu alte dispozitive.
- Licențiere și verificarea stării licențelor.
- Configurarea mediilor virtuale (VM): Windows (7, 10, etc.), și macOS.
- Personalizarea imaginilor VM și actualizarea automată a acestora.
- Setarea tipurilor de fișiere suportate: arhive, executabile, PDF, Office, scripturi, Flash, etc.
- Configurarea modului sniffer pentru protocoale: HTTP, FTP, POP3, IMAP, SMTP, SMB.
- Încărcarea manuală a fișierelor pentru analiză via Web UI/API.
- Integrarea regulilor Yara pentru detecție personalizată.

- Analiza comportamentală: monitorizarea modificărilor OS (registri, apeluri sistem, procese).
- Detecția zero-day și phishing
- Corelația MITRE ATT&CK: interpretarea rapoartelor.
- Configurarea alertelor email pentru detecții malware/atacuri.
- Rapoarte: screenshot-uri, trafic rețea, timeline comportamental, clasificare risc (scăzut/mediu/ridicat).
- Integrarea cu baze de date antivirus.

4. Administrare și Monitorizare

- Utilizarea interfețelor de administrare: Web UI, CLI.
- Monitorizarea resurselor: CPU, memorie, stocare (HDD/SSD).
- Gestionarea log-urilor.
- Actualizări automate: semnături, firmware.
- Export/import configurații și resetare la setările din fabrică.
- Verificarea stării licențelor și a subscripțiilor (36 luni).

5. Integrare și Scalabilitate

- Integrarea cu alte soluții
- Scalabilitate
- Configurarea cu antispam email.

6. Practică Hands-On

- Exercițiu 1: Configurarea inițială a unui echipament (IP, licențe, conectivitate).
- Exercițiu 2: Configurarea unui mediu VM și încărcarea unui fișier pentru analiză.
- Exercițiu 3: Generarea și interpretarea unui raport de detecție (ex. malware zero-day).
- Exercițiu 4: Configurarea alertelor email și monitorizarea log-urilor.

7. Depanare și Suport

- Probleme comune: conectivitate, licențe expirate, VM nefuncționale.
- Depanare: verificarea log-urilor, resetarea configurațiilor, contactarea suportului
- Resurse: portaluri de suport, documentație oficială.
- Backup și restaurare configurații.

8. Concluzii și resurse suplimentare

- Rezumatul funcționalităților și diferențelor între echipamente.
- Recomandări pentru utilizare optimă.

Componenta 2 – „Sistem de protecție pentru soluția de mesagerie electronică” în site-ul Disaster Recovery și Business Continuity (DR/BC), destinat extinderii capacității de apărare cibernetică împotriva amenințărilor specifice serviciilor de poștă electronică, bazat pe soluții de securitate tip appliance destinat protecției antispam și antivirus pentru traficul de mesagerie electronică cu capacități de operare în mod transparent (bridge), gateway (MTA) cu subscripție și suport pe o perioadă de minim 36 luni

1. Caracteristicile tehnice generale:

- număr domenii suportate: minim 1500;
- performanța de rutare mesaje e-mail : minim 2.000.000 mesaje/oră, optimizat pentru volume mari;
- funcționarea în mod “server mode” cu suport pentru “local mailboxes”: minim 3000;
- scanare antispam/antivirus: DA;
- administrare : să suporte conturi ierarhizate și roluri personalizabile;
- reguli antispam/antivirus/conținut: definirea politicilor per domeniu, utilizator sau grup;
- prevenire pierderi de date (DLP): DLP robust/avansat și politici personalizate;
- politici geo-IP: să suporte filtrare bazată pe locație geografică;
- metode administrare: web user interface (HTTP/HTTPS), SSH, CLI;
- integrare cu sisteme existente: compatibil cu office 365 și alte servere SMTP;

2. Funcționalități generale (mod transparent, gateway, server)

- configurare multi-domeniu: să suporte multiple domenii, personalizare / configurare flexibilă;
- mail gateway/outbound: configurabil ca gateway SMTP ;
- rutare bazată pe politici: politici flexibile / avansate (exemplu: rutare, filtrare sau suport VLAN și IP);
- gestiune cozi e-mail: exemplu: gestionarea mesajelor netrimise, amânate, nelivrabile sau liste personalizate);
- politici antispam/antivirus: granulare, suport liste personalizate (exemplu: allow list / block list sau whitelist / blacklist);
- acces carantină: acces carantină per utilizator, sumar zilnic;
- suport SNMP;
- sender reputation list: suport local;
- greylist/regex/SPF/DKIM/domainkeys: suport complet pentru toate;

3. Protecție antivirus/antispayware

- scanare SMTP: scanare completă SMTP, carantină automată;
- notificare înlocuire conținut: Da, notificări personalizabile / configurabile;
- blocare tip fișier: filtrare după extensie, tip sau conținut;
- filtrare atașamente: să suporte politici detaliate;

4. Protecție antispam

- filtrare inbound/outbound: suport complet;
- reguli euristice sau echivalent;
- filtrare conținut/atașamente: filtrare după cuvinte cheie, tipuri de fișiere;
- integrare URI-uri de spam terțe și blacklist în timp real (SURBL/RBL);
- scanare PDF/imagini: să suporte scanarea avansată;
- analiză comportamentală: disponibilă cu subscripția ATP (Advanced Threat Protection) sau echivalent;

5. Criptare:

- S/MIME: suport complet;
- TLS server-to-server: suport standard;

6. Gestiune, logare și raportare

- statistici în timp real: da cu dashboard;
- conturi administrare ierarhizate: suport pentru gestionare centralizată;
- inspecție carantină: acces administrator și utilizator;
- logare modificări/activitate: logare detaliată;
- alerte critice: să fie configurabile;
- rapoarte programate: rapoarte detaliate;

7. Caracteristici hardware

- montare rack: Da;
- surse de alimentare: redundante;
- interfețe RJ-45: minim 4 x 10/100/1000 ethernet RJ-45;
- interfețe echipate cu module SFP+: 2 x 10GB, tip conector LC duplex;
- Stocare: minim 4 TB , hot swappable;
- alimentare: 100-240V, 50-60 Hz;

8. Subscripție și suport

- subscripție ATP (Advanced Threat Protection) sau echivalent: 36 luni, protecție avansată;
- suport de tip Enterprise 24/7 sau echivalent, actualizări automate;

9. Condiții de integrare/conectare

- se va asigura integrarea în clusterul de echipamente existent la nivelul Beneficiarului ce conține următoarele echipamente: 2 X FortiMail 3000F;
- **fără a impacta condițiile de garanție și suport ale soluțiilor/echipamentelor existente.**

10. Condiții privind configurarea

- Se va asigura realizarea configurației astfel încât impactul asupra funcționalităților și sistemelor în producție să fie unul minim.
- Se va asigura configurarea necesară pentru integrarea în clusterul de echipamente existent la nivelul Beneficiarului.
- Se va asigura funcționarea în High Availability activ-pasiv sau activ-activ cu sincronizare de configurație, pentru a nu se afecta funcționalitățile și capabilitățile existente
- Se vor asigura script-uri cu titlu gratuit dacă acestea sunt necesare pentru punerea în funcțiune și operaționalizarea soluției.

11. Transferul de cunoștințe:

1. Configurare inițială:

- Stabilirea domeniilor protejate;- Integrarea cu serverul de mail;
- DNS: adăugare înregistrări MX către gateway, SPF, DKIM, DMARC.

2. Politici de filtrare:

- Setarea regulilor de spam (low, medium, high);
- Politici pentru atașamente (tipuri interzise, scanare sandbox);
- Reguli de DLP (ex: blocare CNP-uri, carduri bancare);
- Whitelist/blacklist IP-uri și domenii.

3. Administrare utilizatori:

- Integrare LDAP/AD (dacă este cazul);
- Creare conturi de utilizatori și administratori;
- Politici diferențiate pe grupuri.

4. Quarantine și raportare:

- Vizualizarea mesajelor blocate;
- Eliberarea mesajelor legitime (false positive);
- Setarea notificărilor automate pentru utilizatori.

5. Monitorizare și alerte:

- Dashboard cu statistici (spam, virus, phishing detectat);
- Alarmer pentru volume neobișnuite;
- Rapoarte periodice trimise prin e-mail.

Factori de evaluare și punctaj

Justificarea criteriului de atribuire și a factorilor de evaluare

Criteriul de atribuire	Motivare alegere criteriu
Cel mai bun raport calitate – preț	Autoritatea contractantă urmărește aplicarea unei proceduri de atribuire care oferă posibilitatea de a fi selectată oferta cea mai avantajoasă din punct de vedere al calității și expertizei tehnice pentru sistemul informatic oferat și, în același timp, care permite încadrarea în limitele bugetului alocat și implementarea eficientă a contractului.

Factori de evaluare	Motivare alegere factori de evaluare
Prețul ofertei	Punctajul maxim de 70 puncte a fost stabilit astfel încât să reflecte în termeni de eficiență economică achiziționarea sistemului care face obiectul procedurii de atribuire. Ofertantul care are prețul unitar cel mai scăzut va primi punctajul maxim. Ceilalți ofertanți vor fi punctați ponderat în funcție de raportul dintre prețul minim oferat și prețul oferat de fiecare ofertant în parte în conformitate cu formula de calcul stabilită.
Perioada de garanție	Echipamentele sau componentele defecte pot fi o cauză a înlocuirii înainte de termen. Acest factor de evaluare oferă un stimulent pentru furnizori pentru a asigura creșterea longevității produselor și pentru a garanta că își vor asuma răspunderea pentru repararea tuturor defectelor. Acest factor de evaluare a fost stabilit deoarece ofertarea de garanție suplimentară implică suplimentarea perioadei privind dreptul de utilizare dar și pentru a garanta asumarea de furnizor a răspunderii pentru repararea tuturor defectelor.
Suport și Subscripție	Patch-urile/Pachetele de update/upgrade pot fi o cauză a unor riscuri de securitate ca urmare a unor vulnerabilități netratate corespunzător în cadrul acestor. Acest factor de evaluare oferă un stimulent pentru furnizori pentru a asigura creșterea calității produselor și pentru a garanta că își vor asuma răspunderea pentru remedierea tuturor vulnerabilităților de securitate. Acest factor de evaluare a fost stabilit deoarece ofertarea suport subscripție suplimentară implică suplimentarea perioadei privind dreptul de utilizare dar și pentru a garanta asumarea de furnizor a răspunderii pentru remedierea tuturor vulnerabilităților de securitate.

$$\text{Punctaj} = P(n) + P_{\text{Tehnic}}$$

Denumire factor evaluare	Descriere	Pondere	Algoritm de calcul
Prețul ofertei	Componenta financiară	70% Punctaj maxim 70	Punctajul se acordă astfel: - Pentru cel mai scăzut dintre prețuri se acordă punctajul maxim alocat. - Pentru celelalte prețuri oferite punctajul $P(n)$ se calculează proporțional, astfel: $P(n) = \left[\frac{\text{Preț}_{\text{minim_ofertat}}}{\text{Preț}(n)} \right] \times 70$ unde $\text{Preț}(n)$ este prețul ofertantului curent.
Propunerea tehnică	Componenta tehnică	30% Punctaj maxim 30	Punctajul $P(g)$ se acordă astfel: $P_{\text{Tehnic}} = P_{go} + P_{so}$ P_{go} – punctaj acordat ofertantului pentru factorul Garanție extinsă acordată produselor P_{so} – punctaj acordat ofertantului pentru factorul Suport și Subscripție Extinsă acordată produselor
Factor Garanție extinsă acordată produselor	Acordarea unei perioade de garanție suplimentară cerinței minime din caietul de sarcini	15% Punctaj maxim 15	Algoritm de calcul punctaj: G_{ofertat} - garanția oferită [în luni] G_{min} = garanție minim acceptată [în luni] (36 luni) G_{max} = garanție maximă menționată [în luni] (72 luni) P_{max} = punctaj maxim (15 puncte) P_{go} = punctaj garanție oferită $P_{go} = \frac{(G_{\text{ofertat}} - G_{\text{min}}) \times P_{\text{max}}}{G_{\text{max}} - G_{\text{min}}} = \frac{(G_{\text{ofertat}} - 36) \times 15}{72 - 36}$ Notă: Perioada de garanție minim acceptată este de 36 luni iar perioada de garanție maximă este de 72 luni. Peste perioada de garanție maximă menționată (72 luni), oferta nu va fi punctată suplimentar, iar sub perioada de garanție minim acceptată, oferta va fi considerată neconformă. În cazul ofertării perioadei de garanție minim solicitată (36 luni) oferta nu va fi punctată, situație în care propunerea tehnică va primi din oficiu 0,01 puncte având în vedere că SEAP nu permite punctaj 0.

Denumire factor evaluare	Descriere	Pondere	Algoritm de calcul
Factor Suport și Subscripție extinsă acordată produselor	Acordarea unei perioade de suport și subscripție suplimentară cerinței minime din caietul de sarcini	15% Punctaj maxim 15	<i>Algoritm de calcul punctaj:</i> $S_{ofertat}$ - Suport și Subscripție oferite [în luni] S_{min} = Suport și Subscripție minim acceptate [în luni] (36 luni) S_{max} = Suport și Subscripție maxime menționate [în luni] (72 luni) P_{max} = punctaj maxim (15 puncte) P_{so} = punctaj perioada de suport și subscripție ofertă $P_{so} = \frac{(S_{ofertat} - S_{min}) \times P_{max}}{S_{max} - S_{min}} = \frac{(S_{ofertat} - 36) \times 15}{36}$ Notă: Perioada de suport și subscripție minim acceptată este de 36 luni iar perioada de suport și subscripție maximă este de 72 luni. Peste perioada de suport și subscripție menționată (72 luni), oferta nu va fi punctată suplimentar, iar sub perioada de suport și subscripție minim acceptată, oferta va fi considerată neconformă. În cazul ofertării perioadei de suport și subscripție minim solicitată (36 luni) oferta nu va fi punctată, situație în care propunerea tehnică va primi din oficiu 0,01 puncte având în vedere că SEAP nu permite punctaj 0.

Nr. Crt.	Nume și prenume	Semnătura
1.	Ana-Maria MIHAI	Mihai Ana-Maria Digitally signed by Mihai Ana-Maria Date: 2026.05.12 10:02:22 +03'00'
2.	Marius Bogdan STAN	Marius Bogdan Stan Digitally signed by Marius Bogdan Stan Date: 2026.05.12 10:41:35 +03'00'

Semnat digital de Iulian
 Dragulin
 Date: 2026.05.13 12:53:51
 +03'00'