

DOCUMENTAȚIA STANDARD
pentru realizarea achizițiilor publice de bunuri și servicii

INSTRUCȚIUNI PENTRU AUTORITĂȚI CONTRACTANTE ȘI OFERTANȚI

Secțiunea 1

Dispoziții generale

1. Prezenta Documentație reprezintă o instrucțiune pentru autoritățile contractante și ofertanți, utilizată la inițierea și desfășurarea procedurilor de achiziții publice de bunuri și servicii. La procedurile de achiziții de bunuri și servicii inițiate și desfășurate prin cererea ofertelor de prețuri și achizițiile de valoare mică, autoritățile contractante pot simplifica formularele în dependență de complexitatea achiziției.

2. Prezenta Documentație conține anexe destinate inițierii, publicării, atribuirii și modificării procedurilor de achiziții publice, precum și destinate să faciliteze elaborarea și prezentarea ofertei, și a documentelor care să permită grupului de lucru examinarea și evaluarea tuturor ofertelor depuse, după cum urmează:

- 1) Anunț de intenție (anexa nr.1);
- 2) Anunț de participare, inclusiv pentru procedurile de preselecție/procedurile negociate (anexa nr. 2);
- 3) Invitație de participare la etapele de preselecție/la procedurile negociate (anexa nr. 3);
- 4) Proces-verbal cu privire la rezultatele preselecției candidaților (anexa nr. 4);
- 5) Anunț de atribuire (anexa nr. 5);
- 6) Anunț privind modificarea contractului de achiziții publice/acordului-cadru (anexa nr. 6);
- 7) Cerere de participare (anexa nr. 7);
- 8) Declarație privind valabilitatea ofertei (anexa nr. 8);
- 9) Scrisoare de garanție bancară (anexa nr. 9);
- 10) Garanția de bună execuție (anexa nr. 10.);
- 11) Informații privind asocierea (anexa nr. 11);
- 12) Declarație privind lista principalelor livrări/prestări efectuate în ultimii 3 ani de activitate (anexa nr. 12);
- 13) Declarație privind dotările specifice, utilajul și echipamentul necesar pentru îndeplinirea corespunzătoare a contractului (anexa nr. 13);
- 14) Declarație privind personalul de specialitate propus pentru implementarea contractului (anexa nr. 14);
- 15) Lista subcontractanților și partea/părțile din contract care sunt îndeplinite de aceștia (anexa nr. 15);
- 16) Angajament terț susținător financiar (anexa nr. 16);
- 17) Declarație terț susținător financiar (anexa nr. 17);
- 18) Angajament privind susținerea tehnică și profesională a ofertantului/grupului de operatori economici (anexa nr. 18);
- 19) Declarație terț susținător tehnic (anexa nr. 19);

- 20) Declarație terț susținător profesional (anexa nr. 20);
- 21) Caiet de sarcini (anexa nr. 21);
- 22) Specificații tehnice (anexa nr. 22);
- 23) Specificații de preț (anexa nr. 23);
- 24) Contract – model (anexa nr. 24);
- 25) Acord adițional (anexa nr. 25);
- 26) Acord-cadru (anexa nr. 26).

3. Detaliile privind cantitățile de bunuri și servicii, specificațiile tehnice, standardele și resursele sunt prezentate în caietul de sarcini (anexa nr. 21).

4. Autoritatea contractantă urmează să se asigure că la momentul inițierii procedurii de achiziție publică, mijloacele financiare sunt alocate sau există o garanție a alocării lor și destinate exclusiv achiziției în cauză.

5. Atribuirea contractului de achiziție publică de bunuri și servicii se realizează în conformitate cu prevederile Legii nr. 131/2015 privind achizițiile publice.

6. În cazul în care autoritatea contractantă inițiază un acord-cadru, ca modalitate specială de atribuire a contractelor de achiziții publice de bunuri și de servicii, procedura se desfășoară conform Regulamentului cu privire la acordul-cadru ca modalitate specială de atribuire a contractelor de achiziții publice, aprobat prin Hotărârea Guvernului nr. 694/2020.

7. În cazul în care autoritatea contractantă inițiază procedura de negociere, procedura se desfășoară conform Regulamentului cu privire la achizițiile publice folosind procedura de negociere, aprobat prin Hotărârea Guvernului nr. 599/2020.

8. În cazul în care autoritatea contractantă inițiază proceduri cu preselecție se utilizează anexele ce țin de procedurile date: anexa nr. 1, anexa nr. 3, anexa nr. 4, anexa nr. 5, anexa nr. 6 și anexa nr. 25.

9. Ofertantul suportă toate costurile asociate elaborării și prezentării ofertei sale, precum și documentelor care o însoțesc.

10. Cererea de participare (anexa nr. 7), Oferta, Documentul Unic de Achiziții European (în continuare - DUAE), documentația de atribuire, caietul de sarcini și toată corespondența dintre ofertant și autoritatea contractantă se întocmește în limba română, sau după caz, toate documentele enumerate pot fi întocmite în una din limbile de circulație internațională. Documentele justificative și literatura de specialitate tipărită, care fac parte din ofertă, pot fi întocmite și în altă limbă, specificată în documentația de atribuire, cu condiția ca acestea să fie însoțite de o traducere exactă a fragmentelor relevante în limba română.

11. În cazul în care autoritatea contractantă a depistat că ofertantul a fost implicat în practicile descrise la pct. 22 și pct. 23 în cadrul procedurii de atribuire pentru contractul de achiziție publică aceasta:

1) exclude ofertantul din procedura respectivă de achiziție și înaintează solicitarea către Agenția Achiziții Publice privind includerea lui în Lista de interdicție, conform prevederilor Hotărârii Guvernului nr. 1420/2016 pentru aprobarea Regulamentului privind evidența Listei operatorilor economici calificați; sau

2) întreprinde orice alte măsuri prevăzute în art. 42 al Legii nr. 131/2015 privind achizițiile publice.

12. Sunt interzise următoarele acțiuni în cadrul procedurii de achiziție:

1) promisiunea sau oferirea unei persoane cu funcție de răspundere, personal sau prin mijlocitor, de bunuri sau servicii, sau privilegii, sau avantaje sub orice formă, pentru a influența acțiunile unei alte părți;

2) orice acțiune sau omisiune, inclusiv interpretare eronată, care, conștient sau din neglijență, induce în eroare sau tinde să inducă în eroare o parte pentru obținerea unui beneficiu financiar sau de altă natură ori pentru a evita o obligație;

3) înțelegerea interzisă de lege, între două sau mai multe părți, realizată în scopul coordonării comportamentului lor la procedurile de achiziții publice;

4) prejudicierea, direct sau indirect, a oricărei părți sau a proprietății acestei părți, pentru a influența în mod necorespunzător acțiunile acesteia;

5) distrugerea intenționată, falsificarea, contrafacerea sau ascunderea materialelor de evidență ale investigării, sau prezentarea unor informații false organelor de urmărire penală, pentru a împiedica esențial urmărirea penală condusă de către organele de resort în vederea identificării unor practici frauduloase, precum și amenințarea, hărțuirea sau intimidarea oricărei părți pentru a o împiedica să divulge informația cu privire la chestiuni relevante urmăririi penale.

Secțiunea a 2-a

Calificarea candidaților/ofertanților

13. Orice operator economic, rezident sau nerezident, persoana fizică sau juridică de drept public sau privat ori asociație de astfel de persoane are dreptul de a participa la procedura de atribuire a contractului de achiziție publică de bunuri și servicii.

14. Persoana fizică sau juridică care a participat la întocmirea documentației de atribuire are dreptul, în calitate de operator economic, de a fi ofertant, ofertant asociat sau subcontractant, dar numai în cazul în care implicarea sa în elaborarea documentației de atribuire nu este de natură să distorsioneze concurența. Persoana fizică sau juridică care participă direct în procesul de verificare și evaluare a ofertelor nu are dreptul de a fi ofertant, ofertant asociat sau subcontractant, sub sancțiunea excluderii din procedura de atribuire.

15. Mai multe persoane juridice au dreptul să se asocieze în scopul depunerii unei oferte comune, de asemenea, fiecare asociat urmează să prezinte DUAE-ul separat. Asocierea trebuie prezentată în formă scrisă la solicitarea autorității contractante, odată ce a fost declarat în DUAE.

16. Filialele agenților economici, cu personalitate juridică și înregistrate în conformitate cu prevederile pct. 29, au dreptul de a participa la procedura de atribuire a contractului de achiziție publică de bunuri și servicii în nume propriu și, în acest scop, trebuie să prezinte documente care dovedesc eligibilitatea, înregistrarea, capacitatea tehnică și capacitatea economico-financiară.

17. Sucursalele au dreptul de a participa la procedura de atribuire a contractului de achiziție publică de bunuri și servicii și de a încheia contractul respectiv numai în numele persoanei juridice, prin împuternicire. În acest caz documentele prezentate, care dovedesc eligibilitatea, înregistrarea, capacitatea tehnică și capacitatea economico-financiară, trebuie să fie cele ale persoanei juridice.

18. Pentru confirmarea datelor de calificare în cadrul procedurii de achiziții publice, operatorul economic completează și prezintă DUAE, conform formularului standard al Documentului unic de achiziții European, aprobat prin Ordinul ministrului finanțelor nr.

72/2020, în conformitate cu cerințele stabilite de autoritatea contractantă. Prezentarea oricărui alt formular DUAE, este temei de descalificare de la procedura de achiziție publică.

19. În dependență de specificul achiziției și procedura aleasă, autoritatea contractantă are obligația de a stabili pentru fiecare procedură în parte criteriile de calificare cât și documentele suport necesare pentru a fi prezentate de către operatorii economici.

20. Autoritatea contractantă aplică criteriile și cerințe de calificare numai referitoare la:

- 1) eligibilitatea ofertantului sau candidatului;
- 2) capacitatea de exercitare a activității profesionale;
- 3) capacitatea economică și financiară;
- 4) capacitatea tehnică;
- 5) standarde de asigurare a calității;
- 6) standarde de protecție a mediului.

21. Pentru constatarea datelor de calificare în cadrul procedurilor de achiziții publice, operatorul economic prezintă la momentul evaluării documentele solicitate de către autoritatea contractantă în cadrul procedurilor de achiziții publice. Documentele se prezintă în format electronic, utilizând Sistemul informațional automatizat “Registrul de stat al achizițiilor publice” (în continuare - SIA RSAP), cu excepția cazurilor prevăzute la art. 33 alin. (7) și alin. (11) din Legea nr. 131/2015 privind achizițiile publice.

22. Se exclude de la procedura de atribuire a contractului de achiziții publice orice ofertant sau candidat despre care se confirmă că, în ultimii 5 ani, a fost condamnat, prin hotărârea definitivă a unei instanțe judecătorești, pentru participare la activități ale unei organizații sau grupări criminale, pentru corupție, pentru fraudă și/sau pentru spălare de bani, pentru infracțiuni de terorism sau infracțiuni legate de activități teroriste, finanțarea terorismului, exploatarea prin muncă a copiilor și alte forme de trafic de persoane.

23. Se exclude de la procedura pentru atribuire a contractului de achiziție publică, și respectiv, nu este eligibil, orice ofertant care se află în oricare dintre situațiile prevăzute la art. 19 alin. (2) și alin. (3) și art. 16 alin. (6) al Legii nr. 131/2015 privind achizițiile publice.

24. Orice ofertant/candidat care se află în una din situațiile menționate la pct. 22 și pct. 23 furnizează dovezi care să arate că măsurile luate de el sunt suficiente pentru a demonstra fiabilitatea și credibilitatea sa, în pofida existenței unui motiv de excludere. Dacă autoritatea contractantă consideră astfel de dovezi suficiente, ofertantul/candidatul în cauză nu este exclus de la procedura de achiziție publică, cu excepția cazului în care operatorul economic a fost exclus prin hotărâre definitivă a unei instanțe de judecată de la participarea la procedurile de achiziții publice.

25. Autoritatea contractantă extrage informația necesară pentru constatarea existenței sau inexistenței circumstanțelor menționate la pct. 22 și pct. 23 în bazele de date disponibile ale autorităților publice sau ale părților terțe. Dacă acest lucru nu este posibil, autoritatea contractantă are obligația de a accepta ca fiind suficient și relevant pentru demonstrarea faptului că ofertantul/candidatul nu se încadrează în una dintre situațiile prevăzute la pct. 22 și pct. 23 orice document considerat edificator, din acest punct de vedere, în țara de origine sau în țara în care ofertantul este stabilit, cum ar fi certificate, caziere judiciare sau alte documente echivalente emise de autorități competente din țara respectivă.

26. În ceea ce privesc referințele de la pct. 23, în conformitate cu legislația internă a statului în care sunt stabiliți ofertanții, aceste solicitări se referă la persoanele fizice și persoanele juridice, inclusiv, după caz, la directori de companii sau la orice persoană cu putere de reprezentare, de decizie ori de control în ceea ce privește ofertantul/candidatul.

27. În cazul în care în țara de origine sau în țara în care este stabilit ofertantul/candidatul nu se emit documente de natura celor prevăzute la pct. 22 sau respectivele documente nu vizează toate situațiile referitoare de la pct. 23, autoritatea contractantă are obligația de a accepta o declarație pe propria răspundere sau, dacă în țara respectivă nu există prevederi legale referitoare la declarația pe propria răspundere, o declarație autentică dată în fața unui notar, a unei autorități administrative sau judiciare sau a unei asociații profesionale care are competențe în acest sens.

28. Autoritatea contractantă evaluează măsurile întreprinse de către operatorii economici ținând seama de gravitatea și circumstanțele particulare ale infracțiunii sau ale abaterii. În cazul în care consideră că măsurile întreprinse sunt insuficiente, autoritatea contractantă informează ofertantul/candidatul despre motivele excluderii.

29. Autoritatea contractantă solicită oricărui ofertant să prezinte dovada din care să rezulte o formă de înregistrare în cazul persoanei juridice, capacitatea legală de a executa documentația de atribuire și de a livra/presta bunurile/serviciile, în conformitate cu prevederile legale din țara în care este stabilit.

30. Ofertantul urmează să dispună de un nivel minim de capacitate economică și/sau financiară și să prezinte informații/documente privind capacitatea economică și/sau financiară pentru a se califica conform cerințelor de îndeplinire a contractului, cum ar fi:

1) realizarea unei cifre medii anuale de afaceri în ultimii 3 ani egală sau mai mare decât suma stabilită în pct. 16 din anexa nr. 2, care nu trebuie să depășească de două ori valoarea estimată a contractului, cu excepția cazurilor bine justificate, precum cele legate de riscurile speciale aferente naturii bunurilor sau serviciilor;

2) declarații bancare corespunzătoare sau, după caz, dovezi privind asigurarea riscului profesional;

3) situația financiară pentru perioada de gestiune anterioară, avizat și înregistrat de organele competente, și orice alte documente legale edificatoare prin care ofertantul își poate dovedi capacitatea economico-financiară.

31. Atunci când un contract este împărțit pe loturi, indicele cifrei de afaceri se aplică pentru fiecare lot individual. Cu toate acestea, autoritatea contractantă urmează să stabilească cifra de afaceri anuală minimă impusă operatorilor economici cu referire la grupuri de loturi, dacă ofertantului câștigător îi sunt atribuite mai multe loturi care trebuie executate în același timp.

32. La solicitarea autorității contactante, ofertantul urmează să prezinte documentele care demonstrează capacitatea tehnică și/sau profesională pentru executarea viitorului contract numai în măsura în care aceste informații sînt relevante pentru îndeplinirea contractului și nu sînt disponibile în bazele de date ale autorităților publice sau ale părților terțe:

1) o listă a principalelor livrări de bunuri/servicii similare efectuate în ultimii 3 ani, conform Anexei nr. 12. Respectivul certificări indică beneficiarii, indiferent dacă aceștia sunt autorități contractante sau clienți privați, valorile și perioadele de livrare/prestare.

2) declarația referitoare la echipamentele tehnice și la măsurile aplicate în vederea asigurării calității, precum și, dacă este cazul, la resursele de studiu și cercetare;

3) informații referitoare la personalul/organismul tehnic de specialitate de care dispune sau al cărui angajament de participare a fost obținut de către ofertant/candidat, în special pentru asigurarea controlului calității;

4) certificate sau alte documente emise de organisme abilitate în acest sens, care să ateste conformitatea bunurilor, identificată clar prin referire la specificații sau standarde relevante;

5) mostre (în măsura în care necesitatea prezentării este justificată), descrieri și/sau fotografii a căror autenticitate trebuie să poată fi demonstrată în cazul în care autoritatea contractantă solicită acest lucru;

6) informații referitoare la studiile, pregătirea profesională și calificarea personalului de conducere, precum și ale persoanelor responsabile pentru îndeplinirea contractului conform Anexei nr. 14;

7) declarația referitoare la efectivele medii anuale ale personalului angajat și ale cadrelor de conducere în ultimii 3 ani;

8) dacă este cazul, informații privind măsurile de protecție a mediului pe care operatorul economic le poate aplica în timpul îndeplinirii contractului de bunuri/servicii, în corespundere cu pct. 36;

9) informații referitoare la utilajele, instalațiile, echipamentele tehnice de care dispune operatorul economic pentru îndeplinirea corespunzătoare al contractului de bunuri/servicii conform Anexei nr. 13;

10) informații privind partea din contract pe care operatorul economic are, eventual, intenția să o subcontracteze, conform Anexei nr. 15. De asemenea, urmează a fi atașat/atașate la Anexa nr. 15, copia/copiile contractului/contractelor încheiat/încheiate cu subatreprenorii.

33. Ofertantul urmează să dispună de un nivel minim de experiență pentru a se califica conform cerințelor de îndeplinire a contractului prin demonstrarea experienței specifice fiind minimum de 3 ani în livrarea/prestarea bunurilor/serviciilor similare, confirmată prin anexarea copiilor contractelor, facturilor și actelor de primire-predare.

34. Operatorul economic urmează să prezinte, în cazul solicitării din partea autorității contactante, documente și certificate emise de organisme independente, prin care se atestă faptul că respectă anumite standarde de asigurare a calității (ISO 9001), acestea trebuie să se raporteze la sistemele de asigurare a calității, bazate pe seriile de standarde europene relevante, certificate de organisme conforme cu seriile de standarde europene privind certificarea, sau la standarde internaționale pertinente, emise de organisme acreditate.

35. În conformitate cu principiul recunoașterii reciproce, autoritatea contractantă are obligația de a accepta certificatele echivalente emise de organismele stabilite în statele membre ale Uniunii Europene. În cazul în care operatorul economic nu deține un certificat de calitate astfel cum este solicitat de autoritatea contractantă, aceasta din urmă are obligația de a accepta orice alte certificări prezentate de operatorul economic respectiv, în măsura în care acestea confirmă asigurarea unui nivel corespunzător al calității.

36. Operatorul economic prezintă documente, certificate, emise de organisme independente, prin care se atestă faptul că respectă anumite standarde de protecție a mediului, aceasta trebuie să se raporteze:

1) la Sistemul Comunitar de Management de Mediu și Audit (EMAS), sau;

2) la standarde de gestiune ecologică bazate pe seriile de standarde europene sau internaționale în domeniu, certificate de organisme conforme cu legislația comunitară ori cu standardele europene sau internaționale privind certificarea.

37. În conformitate cu principiul recunoașterii reciproce, autoritatea contractantă are obligația de a accepta certificatele echivalente emise de organismele stabilite în statele membre ale Uniunii Europene. În cazul în care operatorul economic nu deține un certificat de mediu astfel cum este solicitat de autoritatea contractantă, aceasta din urmă are obligația de a accepta orice alte certificări prezentate de operatorul economic respectiv, în măsura în care acestea confirmă asigurarea unui nivel corespunzător al protecției mediului.

38. Autoritățile contractante pot utiliza o serie de criterii generale privind durabilitatea pentru livrarea bunurilor și prestarea serviciilor:

1) Etichetele cu criterii multiple: eticheta europeană (floarea), eticheta scandinavă (lebedă nordică) și etichetele naționale (precum îngerul albastru german);

2) Achiziționarea alimentelor organice și cu un aport nutrițional echilibrat pentru școli/grădinițe;

3) Posibilitățile de reciclare/reutilizare a produsului după scoaterea din uz a acestuia;

4) Folosirea de recipiente sau ambalaje reutilizabile pentru transportarea produselor;

5) Furnizarea de hârtie ecologică și reciclată (fără clor și fibră);

6) Restricțiile de utilizare a anumitor substanțe periculoase în compoziția produsului;

7) Sisteme eficiente de tratare a deșeurilor în aer și în apă în fabricarea produselor;

8) Utilizarea sistemelor și schemelor de management de mediu (de exemplu EMAS, ISO 14001);

9) Reducere ale emisiilor de CO₂ și a altor gaze prin scăderea frecvenței livrării și opțiuni noi de ambalare;

10) Reciclarea sau reutilizarea ambalajelor care însoțesc produsele;

11) Introducerea specificațiilor pentru vehicule cu cel mai mic nivel posibil de emisii de CO₂ pentru categoria și dimensiunile respective, standarde EURO privind emisiile de particule și de Nox;

12) Încurajarea utilizării vehiculelor cu combustibili alternativi și a variantelor electrice sau hibride;

13) Achiziționarea vehiculelor cu sisteme de aer condiționat cu agenți de răcire cu nivel scăzut de GWP (potențial de încălzire globală);

14) Achiziționarea echipamentelor/utilajelor din clasa de eficiență energetică cea mai ridicată;

15) Achiziționarea corpurilor de iluminat cu un conținut scăzut de mercur;

16) Reducerea poluării aerului în orașe (prin achiziția de autobuze și automobile cu nivel scăzut al emisiilor de pulberi în suspensie și oxizi de azot);

17) Achiziționarea de alimente organice și nemijlocit susținerea agriculturii durabile;

18) Economisirea resurselor naturale (prin achiziția de produse obținute din materiale reciclate, reducerea consumului de hârtie prin achiziționarea, promovarea utilizării dispozitivelor multifuncționale);

19) Achiziționarea de materiale de construcție și aprovizionare durabilă;

20) Încurajarea utilizării de materiale reciclate în construcție;

21) Aprovizionarea cu produse certificate ca fiind durabile (Patru etichete ecologice ale UE pentru componente);

22) Achiziționarea și utilizarea de materiale de construcție cu impact redus asupra mediului;

23) Serviciile pentru depozitarea deșeurilor reciclabile și sistemul de gestionare a deșeurilor;

24) Gestionarea deșeurilor din demolări;

25) Achiziționarea serviciilor de curățenie ecologică folosind produse care întrunesc cerințele etichetelor ecologice;

26) Achiziționarea serviciilor de catering cu alimente ecologice (bio), indicând procentul de alimente ecologice;

27) Utilizarea unui sistem de management de mediu (EMS) pentru servicii de catering;

28) Utilizarea de metode non-chimice, care respectă mediul;

29) Achiziționarea de energie electrică ecologică;

30) Impunerea unor durate de viață prelungite ale produselor și a unei garanții pentru piesele de schimb;

31) și altele.

39. În cazul unei asocieri, cerințele solicitate pentru îndeplinirea criteriilor de calificare și de selecție referitoare la situația economică și financiară sau a capacităților tehnice și profesionale pot fi îndeplinite prin cumul proporțional sarcinilor ce le revin fiecărui asociat.

40. În ceea ce privește criteriile privind cifra de afaceri, în cazul unei asocieri, cifra de afaceri medie anuală luată în considerare este valoarea generală, rezultată prin însumarea cifrelor de afaceri medii anuale corespunzătoare fiecărui membru al asocierii.

41. În ceea ce privește experiența, pentru a se califica conform cerințelor stabilite, asociațiile trebuie să demonstreze o experiență proporțională sarcinilor ce revin fiecărui asociat.

42. Capacitatea economică și financiară, cât și capacitatea tehnică și/sau profesională a ofertantului/candidatului poate fi susținută, pentru îndeplinirea unui contract, și de o altă persoană, indiferent de natura relațiilor juridice existente între ofertant/candidat și persoana respectivă.

43. În cazul în care ofertantul/candidatul își demonstrează capacitatea economică și financiară cât și capacitatea tehnică și/sau profesională invocând și susținerea acordată, în conformitate cu prevederile pct. 42 de către o altă persoană, acesta are obligația de a dovedi susținerea de care beneficiază prin prezentarea în formă scrisă a unui angajament ferm al persoanei respective, încheiat în formă autentică (conform anexelor nr. 16 și nr. 18) și declarațiile terțului susținător financiar și terțului susținător tehnic și profesional (anexele nr. 17, nr. 19 și nr. 20), prin care această persoană confirmă faptul că pune la dispoziția ofertantului/candidatului resursele financiare cât și resurse tehnice și profesionale invocate. Prezentarea angajamentului se face la solicitarea autorității contractante odată ce a fost declarat în DUAE. Persoana care asigură susținerea financiară cât și tehnică și profesională trebuie să îndeplinească criteriile de selecție relevante și nu trebuie să se afle în niciuna dintre situațiile prevăzute la pct. 22 și pct. 23 care determină excluderea din procedura de atribuire.

Secțiunea a 3-a

Pregătirea/Elaborarea ofertelor

44. Autoritatea contractantă în caietul de sarcini descrie condițiile/cerințele de furnizare:

a) a energiei electrice, în conformitate cu Legea nr. 174/2017 cu privire la energetică și actele normative de reglementare adoptate de către Consiliul de administrație al Agenției Naționale pentru Reglementare în Energetică (în continuare – ANRE), de exemplu: Regulamentul privind furnizarea energiei electrice, aprobat prin Hotărârea ANRE nr. 23/2017, Regulamentul privind racordarea la rețele electrice și prestarea serviciilor de transport și de distribuție a energiei electrice, aprobat prin Hotărârea ANRE nr. 168/2019, Metodologia de calculare, aprobare și aplicare a tarifelor reglementate pentru serviciile auxiliare prestate de operatorii de sistem din sectorul electroenergetic, aprobată prin Hotărârea ANRE nr. 269/2018, Instrucțiunea privind calcularea pierderilor de energie electrică activă și reactivă în elementele de rețea aflate la balanța consumatorului, aprobată prin Hotărârea ANRE nr. 246/2007, Instrucțiunea privind calcularea consumului tehnologic de energie electrică în rețelele de distribuție, în funcție de valoarea factorului de putere în instalațiile de utilizare, aprobată prin Hotărârea ANRE nr. 89/2003 etc.

b) a gazelor naturale în conformitate cu Legea nr. 108/2016 cu privire la gazele naturale și Legea nr. 174/2017 cu privire la energetică și actele normative de reglementare ale ANRE, de exemplu: Regulamentul privind furnizarea gazelor naturale, aprobat prin Hotărârea ANRE nr. 113/2019.

c) a energiei termice în conformitate cu Legea nr. 92/2014 cu privire la energia termică și promovarea cogenerării și Legea nr. 174/2017 cu privire la energetică, și actele normative de reglementare ale ANRE, de exemplu: Regulamentul privind furnizarea energiei termice, aprobat prin Hotărârea ANRE nr. 169/2019.

d) a alimentării cu apă și canalizare în conformitate cu Legea nr. 303/2013 privind serviciul public de alimentare cu apă și de canalizare și actele normative secundare, de exemplu: Regulamentul-cadru de organizare și funcționare a serviciului public de alimentare cu apă și de canalizare, aprobat prin Hotărârea ANRE nr. 355/2019 sau Regulamentele de organizare și funcționare a serviciului public de alimentare cu apă și de canalizare aprobate de autoritățile publice locale de nivelul întâi, în cazul în care au fost elaborate și aprobate.

e) a produselor petroliere pentru alimentarea automobilelor conform listei complete privind rețeaua de distribuție la nivelul țării din care să rezulte ca ofertantul deține stații de alimentare în localitățile indicate în documentația de atribuire. Carburantul se livrează la stația de alimentare în baza cardurilor emise de către Furnizor. Ofertantul oferă autorității contractante posibilitatea de a achiziționa carburant (fără plată în numerar) prin intermediul cardurilor valorice la stațiile de alimentare ale furnizorului la nivelul fiecăreia dintre localitățile menționate în documentația de atribuire. În cazul în care locul destinației finale îl constituie mai multe localități/regiuni, atribuirea contractelor de achiziție se realizează pe loturi pentru fiecare localitate/regiune în parte. Livrarea cardurilor se face pe baza unei cereri de emisie de card din partea autorității contractante. Termenul solicitat pentru livrarea cardurilor la sediul autorității contractante este de 5 zile lucrătoare de la data intrării în vigoare a contractului și, respectiv, de la data transmiterii cererii de emisie de carduri suplimentare.

45. Autoritatea contractantă în caietul de sarcini precizează detalii privind modul de transportare, prestare, utilizare a produselor/serviciilor:

a) produselor petroliere pentru alimentarea automobilelor

Furnizorul acordă permanent achizitorului posibilitatea accesării on-line a informațiilor privind situația detaliată a tuturor achizițiilor de carburant efectuate de către fiecare autovehicul al său. Posibilitatea achizitorului de a obține la orice stație de distribuție pe bază de card, informații privind valoarea rămasă pentru fiecare card în parte. Furnizorul gestionează lista cardurilor pierdute sau furate și are obligația să blocheze/deblocheze utilizarea acestora în cel mult 24 ore de la solicitarea achizitorului. Furnizorul are obligația de a garanta că produsele furnizate respectă standardele minime de poluare aprobate conform legislației naționale și pot fi alimentate de la stațiile existente în localitățile indicate în documentația de atribuire. Carburanții livrați trebuie să corespundă calitativ normelor în vigoare. Se prezintă în partea II, Condițiile Speciale a Contractului, cât și în anexa nr.1 la Contract „Specificații Tehnice”, condițiile tehnice de calitate și metodele de determinare a produselor, având la bază standarde și omologări naționale sau internaționale. Furnizorul asigură personalizarea cardurilor pe fiecare autovehicul (pe număr de înmatriculare), configurarea cardului pe tipul carburantului. Furnizorul asigură asistență permanentă 24 h, 7 zile din săptămână, pentru ca, în cazul apariției anumitor deficiențe în funcționarea cardurilor pentru carburant, Furnizorul să fie în măsură să soluționeze problemele apărute în cel mai scurt timp posibil. Furnizorul specifică dacă toate cardurile sunt acceptate la toate stațiile PECO situate în localitățile menționate în documentația de atribuire. Furnizorul pune la dispoziția achizitorului instrucțiuni de folosire a cardului. Autoritatea contractantă își rezervă dreptul de a mări sau micșora numărul de carduri și de a suplimenta sau diminua cantitatea de carburanți în baza prevederilor normative.

b) de furnizare a energiei electrice

Evidența consumului de energie electrică se efectuează prin intermediul echipamentului de măsurare al Beneficiarului care este responsabil de integritatea acestuia. În cazul în care echipamentul de măsurare este instalat în limitele proprietății operatorului de sistem, responsabil de integritatea echipamentului de măsurare și a sigiliilor aplicate este operatorul de sistem. Operatorul de sistem asigură, la solicitare, accesul Beneficiarului la echipamentul de măsurare. În acest caz, Beneficiarul este în drept să aplice sigiliul său echipamentului de măsurare. Lucrările de instalare, exploatare, deservire, reparare, verificare metrologică periodică și de înlocuire a echipamentului de măsurare al Beneficiarului se efectuează în conformitate cu Legea nr. 174/2017 cu privire la energetică și Legea nr. 107/2016 cu privire la energia electrică, iar cheltuielile se suportă de către Beneficiar. Controlul echipamentului de măsurare și al sigiliilor aplicate acestuia se efectuează de către operatorul de sistem, după necesitate, și numai în prezența reprezentantului Beneficiarului. Citirea indicilor echipamentului de măsurare în scopul facturării energiei electrice consumate de Beneficiar, se efectuează de operatorul de sistem lunar. Personalul operatorului de sistem și utilizatorul de sistem sunt în drept să stabilească, de comun acord, timpul efectuării activităților pentru citirea indicilor echipamentului de măsurare. Cantitatea energiei electrice furnizate Beneficiarului se determină în baza indicilor echipamentului de măsurare, citite la fiecare loc de consum, sau, în cazurile prevăzute în Regulamentul pentru furnizarea energiei electrice, se calculează prin estimare. În cazul deteriorării echipamentului de măsurare sau dacă se constată încălcarea de către Beneficiar a prevederilor Legii cu privire la energia electrică, care a dus la consum de energie electrică prin evitarea echipamentului de măsurare, prin denaturarea indicațiilor echipamentului de măsurare sau alte modalități de consum neînregistrat de echipamentul de măsurare, contravaloarea energiei electrice consumate se calculează în conformitate cu prevederile Regulamentului pentru furnizarea energiei electrice. Contravaloarea pierderilor de energie electrică în transformatoarele de forță și în liniile electrice ce aparțin Beneficiarului, se calculează în baza Instrucțiunii privind calcularea pierderilor de energie electrică activă și reactivă în elementele de rețea aflate la balanța consumatorului, aprobată prin Hotărârea ANRE nr. 246/2007.

46. Autoritatea contractantă în caietul de sarcini precizează modalitatea de calculare a costului/prețului bunului/serviciului, prin trimitere la actele normative din domeniu.

a) a produselor petroliere pentru alimentarea automobilelor

Prețul unui litru de carburant oferat va fi cel afișat la stațiile de alimentare ale ofertantului cu aplicarea discount-ului oferat.

Furnizorul asigură autorității contractante posibilitatea de a stabili limite individuale valorice pentru fiecare card, inclusiv de a le modifica în sensul majorării sau micșorării acestora. Prețul unitar oferat constituie prețul mediu calculat de către ofertant utilizând prețurile afișate la panourile informative în toate stațiile din localitate/regiune indicate în documentația de atribuire, în decurs de 15 zile până la data publicării anunțului de participare în Buletinul achizițiilor publice, la care se aplică un discount.

Calcularea prețului unitar se efectuează conform formulei:

$$P_u = \frac{(M_1 + M_2 + \dots + M_{15})}{15} - D\%$$

Unde,

P_u – reprezintă prețul unitar oferat;

M_1 – reprezintă media prețurilor afișate la **toate stațiile din localitatea/regiunea specificată în pct. 1** pentru prima zi;

M_2 – reprezintă media prețurilor afișate la **toate stațiile din localitatea/regiunea specificată în pct. 1** pentru a doua zi;

M₁₅ – reprezintă media prețurilor afișate la **toate stațiile din localitatea/regiunea specificată în pct. 1** pentru a cincisprezecea zi;

D% – reprezintă discount-ul aplicat.

Discount-ul este specificat expres în ofertă și ulterior în anexa nr. 2 la contract, rămânând neschimbat pe întreaga perioadă de valabilitate al acestuia. Propunerea financiară este însoțită obligatoriu de documentele confirmative cu privire la prețurile prezentate (bon fiscal). Furnizorul facturează contravaloarea produselor la sfârșitul fiecărei luni, pentru consumul efectuat, conform unei centralizări cu cantitatea alimentată pe fiecare autovehicul în parte. Factura aferentă consumului înregistrat pe fiecare card în parte este însoțită de un raport de consum care conține informații detaliate cu privire la tranzacțiile efectuate pe fiecare card și mașină, locație, dată, ora alimentării, tipul carburantului și, după caz, subtotalul cardului și totalul general de carburant după fiecare tranzacție.

În cazul procurării produselor petroliere pentru alimentarea automobilelor, în conformitate cu art. 26 al Legii nr.131/2015 privind achizițiile publice, se aplică criteriul cel mai bun raport calitate-preț, din care factorul de evaluare prețul, constituie minimum 60%, iar restul factorilor sunt la decizia autorității contractante (ex: discount-ul, amplasarea stațiilor PECO, etc.).

În restul cazurilor ce țin de achiziționarea de carburanți lichizi și/sau gazoși în vrac, uleiuri, etc. se utilizează principiul general de procurare a bunurilor.

b) a energiei electrice

Consumul tehnologic de energie electrică, cauzat de factorul de putere din instalațiile electrice ale Beneficiarului se facturează numai în cazul în care factorul de putere $\cos \varphi$, calculat în punctul de delimitare, este mai mic de _____ (0,92 pentru instalația de utilizare racordată la tensiunea 0,4 kV și 0,87 la tensiunea 10(6) kV). Cantitatea consumului tehnologic de energie electrică, cauzat de factorul de putere din instalațiile electrice ale Beneficiarului se calculează în baza Instrucțiunii privind calcularea consumului tehnologic de energie electrică în rețelele de distribuție, în funcție de valoarea factorului de putere în instalațiile de utilizare, aprobată prin Hotărârea Consiliului de administrație al Agenției nr.89 din 13/2003. În cazul în care furnizorul calculează prețul reieșind din tariful ANRE minus – discount-ul, modul de calculare a prețului se indică în condițiile speciale a contractului și de asemenea se indică și cazurile de modificare a lui. Micșorarea și/sau majorarea prețului și valorii contractului se efectuează prin acord adițional la contract.

47. Operatorul economic interesat de a participa la procedura de achiziție publică este obligat să depună până la expirarea termenului-limită stabilit de către autoritatea contractantă, în acest sens, o cerere de participare, în cazul aplicării prevederilor art. 33 alin. (7) și alin. (11) al Legii nr. 131/2015. În celelalte cazuri, aceasta se depune odată cu oferta.

48. Oferta cuprinde următoarele formulare:

1) Propunerea tehnică - ofertantul elaborează propunerea tehnică, astfel încât aceasta să respecte în totalitate cerințele de calificare, precum și cerințele prevăzute în caietul de sarcini. Propunerea tehnică conține -Specificații tehnice (anexa nr. 22);

2) Propunerea financiară- ofertantul elaborează propunerea financiară, astfel încât aceasta să furnizeze toate informațiile solicitate cu privire la prețuri, tarife, precum și la alte condiții financiare și comerciale legate de obiectul contractului de achiziție publică de bunuri și servicii. Propunerea financiară conține - Specificații de preț (anexa nr.23);

3) DUAE;

4) Garanția pentru ofertă, după caz (anexa nr.9).

49. Toate documentele menționate la pct. 48 se completează fără nici o modificare sau abatere de la formulare, spațiile goale fiind completate cu informația solicitată. Completarea defectuoasă a formularelor atrage respingerea ofertei.

50. Operatorii economici pregătesc ofertele conform cerințelor stabilite în anunțul de participare, publicat de către autoritatea contractantă în Buletinul achizițiilor publice, și depun ofertele în mod electronic, folosind fluxurile interactive de lucru puse la dispoziție de platformele electronice, cu excepția cazurilor prevăzute la art. 33 alin. (7) și alin. (11) din Legea nr. 131/2015 privind achizițiile publice.

51. Ofertantul depune garanția pentru ofertă conform prevederilor Legii nr. 131/2015 privind achizițiile publice.

52. În cazul unei asocieri, garanția pentru ofertă se depune de liderul asociației.

53. Ofertantul are obligația, prin depunerea declarației privind valabilitatea ofertei (anexa nr. 8), de a menține oferta valabilă pe toată perioada de valabilitate prevăzută în documentația de atribuire. Termenul valabilității ofertei începe să decurgă din momentul termenului limită de depunere a ofertelor. Orice ofertă valabilă pentru o perioadă mai mică decât cea prevăzută în anexa nr. 2 se respinge de către grupul de lucru ca fiind necorespunzătoare.

54. În cazul extinderii perioadei de valabilitate a ofertei, perioada de valabilitate a garanției pentru ofertă se prelungește în mod corespunzător.

55. Ofertantul are obligația de a comunica autorității contractante dacă este sau nu este de acord cu prelungirea perioadei de valabilitate a ofertei. Ofertantul care nu este de acord cu prelungirea perioadei de valabilitate a ofertei se consideră că și-a retras oferta, fără ca acest fapt să atragă pierderea garanției pentru ofertă.

56. Ofertele care conțin o perioadă de garanție mai mică decât perioada de valabilitate a ofertelor prevăzută în anexa nr. 2 se resping de către grupul de lucru sau, după caz, specialistul certificat în domeniul achizițiilor publice.

57. Autoritatea contractantă stabilește perioada maximă de livrare/prestare a bunurilor/serviciilor în anexa nr. 2.

58. Prețurile pentru bunurile/serviciile solicitate se indică în lei moldovenești, cu două cifre după virgulă, cu excepția cazurilor în care anexa nr. 2 prevede altfel.

Secțiunea a 4-a

Depunerea și deschiderea ofertelor

59. Oferta scrisă și semnată în format electronic, de către administratorul companiei indicat în Extrasul Registrului de Stat al persoanelor juridice sau de către persoana împuternicită atât și în cazul delegării sau împuternicirii persoanei, la ofertă se anexează actul/documentul de împuternicire și se prezintă conform cerințelor expuse în anexa nr. 2 în conformitate cu instrumentele existente în SIA RSAP, cu excepția cazurilor prevăzute la art. 33 alin. (7) și alin. (11) din Legea nr. 131/2015 privind achizițiile publice.

60. Ofertantul trebuie să ia toate măsurile, astfel încât oferta să fie recepționată și înregistrată în SIA RSAP până la data limită pentru depunerea ofertelor, ținând cont de timpul necesar pentru încărcarea ofertei în sistem. În cazul prezentării ofertelor pe suport de hârtie, autoritatea contractantă eliberează operatorului economic, în mod obligatoriu, o recipisă în care indică data și ora recepționării ofertei.

61. Documentele justificative în sprijinul informațiilor declarate în DUAE, care conțin date cu caracter personal, se prezintă separat, pe suport de hârtie sau în formă scanată, cu aplicarea semnăturii electronice, utilizând mijloace electronice de comunicare sau alte mijloace la etapa evaluării ofertelor, la solicitarea autorității contractante.

62. SIA RSAP nu acceptă ofertele transmise după expirarea termenului limită de depunere a ofertelor.

63. În cazurile prevăzute la art. 33 alin. (7) și alin. (11) din Legea nr. 131/2015 privind achizițiile publice, ofertele depuse după termenul limită de deschidere a ofertelor se înregistrează de către autoritatea contractantă și se restituie ofertantului, fără a fi deschise.

64. În cazul asocierii conform pct. 15, fiecare dintre aceștia își asumă obligația pentru oferta comună și răspunde pentru orice consecințe ale viitorului contract de achiziție publică. Informația privind asocierea se prezintă completând anexa nr. 11.

65. Ofertantul nu are dreptul de a depune decât o singură ofertă de bază. Ofertanții asociați nu au dreptul de a depune alte oferte, în mod individual, pe lângă oferta comună. Ofertele alternative se depun numai dacă autoritatea contractantă a precizat explicit în anunțul de participare că permite sau solicită depunerea de oferte alternative.

66. Persoanele juridice nominalizate ca subcontractanți în cadrul uneia sau mai multor oferte nu au dreptul de a depune oferta în nume propriu sau în asociere.

67. Ofertantul are dreptul să modifice sau să retragă oferta înainte de expirarea termenului de depunere a ofertelor, fără a pierde dreptul de retragere a garanției pentru ofertă.

Secțiunea a 5-a

Evaluarea și compararea ofertelor

68. În cazul în care ofertele conțin secrete tehnice, comerciale sau țin de protecția proprietății intelectuale, autoritatea contractantă asigură păstrarea confidențialității asupra conținutului ofertei, precum și asupra oricărei informații privind ofertantul și totodată, asigură dreptul operatorului economic de a nu face publice aceste date prin aplicarea art. 33 alin. (7) și alin. (11) al Legii nr. 131/2015 privind achizițiile publice, însă aplicarea acestui articol se referă numai la partea ce conțin datele enumerate mai sus.

69. Examinarea documentelor de către autoritatea contractantă se efectuează în baza informațiilor prezentate de către operatorii economici în DUAE, și conform cerințelor stipulate în anunțul de participare prin care menționează că:

1) este eligibil să participe la procedurile de achiziții publice și nu există motive de excludere din cadrul procedurilor de achiziții publice pentru atribuirea contractului de achiziție publică;

2) îndeplinește criteriile referitoare la situația economică și financiară și/sau capacitatea tehnică și profesională stabilite de autoritatea contractantă în anunțul de participare sau în documentația de atribuire.

3) se obligă să asigure și să respecte standardele de asigurare a calității și standardele de protecție a mediului.

70. DUAE a operatorilor economici se verifică după caz, direct de către autoritatea contractantă prin procedurile automate desfășurate în SIA RSAP, prin accesarea unei baze de date a autorităților publice sau a terților din Republica Moldova, iar atunci când este necesar și în alte state.

71. În cazul în care la evaluare se stabilesc discrepanțe între informațiile prezentate de către operatorul economic în DUAE și cerințele stabilite de către autoritatea contractantă, operatorul economic se descalifică, ceea ce duce la respingerea ofertei, fiind stabilită ca inacceptabilă și neconformă, și se examinează documentele următorului ofertant/candidat.

72. Operatorul economic a cărui informație prezentată în DUAE corespunde cerințelor/condițiilor specificate de către autoritatea contractantă în anunț/invitația de participare are obligația să prezinte la cerere și fără întârziere documentele justificative.

73. Ofertantul clasat pe primul loc după aplicarea criteriului de atribuire prezintă documentele justificative prin care să demonstreze că îndeplinește în totalitate cerințele corespunzătoare criteriilor de calificare și de selecție, în conformitate cu informațiile cuprinse în DUAE, cu excepția procedurilor desfășurate în mai multe etape, când documentele justificative sunt solicitate înainte de transmiterea invitațiilor pentru etapa a doua către candidații selectați.

74. Ofertele se examinează de către grupul de lucru creat de autoritatea contractantă sau, după caz, specialistul certificat în domeniul achizițiilor publice.

75. Grupul de lucru sau, după caz, specialistul certificat în domeniul achizițiilor publice are obligația de a stabili care sunt clarificările necesare pentru evaluarea fiecărei oferte, precum și perioada acordată pentru transmiterea clarificărilor.

76. În cazul unei oferte care are un preț anormal de scăzut în raport cu prețul estimat al achiziției, autoritatea contractantă are obligația de a efectua controlul calculării elementelor prețului și de a verifica și anumite elemente ale propunerii financiare stabilite ca fiind cu preț anormal de scăzut cât și respectarea de către ofertant a cerințelor tehnice indicate în caietul de sarcini, și de a solicita în scris, și înainte de a lua o decizie de respingere a acelei oferte, detalii și precizări pe care le consideră relevante cu privire la ofertă, precum, și de a verifica răspunsurile care justifică prețul respectiv.

77. Grupul de lucru sau, după caz, specialistul certificat în domeniul achizițiilor publice respinge oferta în oricare dintre următoarele cazuri:

- 1) ofertantul nu îndeplinește cerințele de calificare și de selecție;
- 2) oferta nu respectă cerințele prevăzute în documentația de atribuire pentru elaborarea și prezentarea ofertelor;
- 3) ofertantul nu transmite în perioada stabilită clarificările solicitate;
- 4) oferta financiară nu are un preț fixat;
- 5) ofertantul modifică, prin clarificările pe care le prezintă, conținutul propunerii tehnice și/sau al propunerii financiare, cu excepția situației în care modificarea este determinată de corectarea erorilor aritmetice sau abaterilor neînsemnate;
- 6) oferta este anormal de scăzută potrivit art. 70 al Legii nr. 131/2015 privind achizițiile publice;
- 7) atunci când explicațiile prezentate de ofertant, la solicitarea autorității contractante, nu sunt concludente și/sau nu sunt susținute de documentele justificative cerute de către grupul de lucru sau, după caz, specialistul certificat în domeniul achizițiilor publice;
- 8) s-a constatat comiterea unor acte de corupție, acte conexe actelor de corupție sau fapte coruptibile confirmate prin hotărâre definitivă a instanței de judecată.

78. Dacă oferta, inclusiv formularele care o însoțesc, nu corespunde cerințelor prestabilite în invitația/anunțul de participare, inclusiv în documentația de atribuire sau aceasta nu este completată, semnată electronic și după caz, semnată și ștampilată în modul corespunzător, ea

se respinge de către autoritatea contractantă, și nu poate fi rectificată cu scopul de a corespunde cerințelor, prin corectarea sau extragerea devierilor sau rezervelor necorespunzătoare, excepție constituind doar corectarea greșelilor aritmetice sau abaterilor neînsemnate.

79. Autoritatea contractantă poate, la discreția sa, să ceară oricăruia dintre ofertanți o clarificare a ofertei acestora, pentru a facilita examinarea, evaluarea și compararea ofertelor. Nu se solicită, nici nu se permit schimbări în prețurile sau în conținutul ofertei, cu excepția corectării erorilor aritmetice descoperite de către autoritatea contractantă în timpul evaluării ofertelor.

80. Erorile aritmetice se corectează după cum urmează: dacă există o discrepanță între prețul pentru o unitate de măsură și prețul total (care este obținut prin multiplicarea prețului cu cantitatea totală), se ia în considerare prețul pe unitate, iar prețul total este corectat în mod corespunzător.

81. Grupul de lucru, după caz, specialistul certificat în domeniul achizițiilor publice are dreptul de a corecta erorile aritmetice numai cu acceptul ofertantului. Dacă ofertantul nu acceptă corectarea acestor erori, oferta sa se consideră necorespunzătoare și, în consecință, se respinge de către grupul de lucru.

82. Operatorul economic este obligat să răspundă la solicitarea de clarificare a autorității contractante în cel mult 3 zile lucrătoare sau, în cazul în care procedura folosită este cererea ofertelor de prețuri, cel mult o zi lucrătoare de la data expedierii acesteia, iar în cazul în care ofertantul nu suplimentează, nu prezintă clarificări sau nu completează informațiile sau documentele solicitate de autoritatea contractantă în termenele stabilite de aceasta, oferta se respinge și se selectează următoarea după clasament dintre ofertele rămase în vigoare.

83. Oferta care corespunde tuturor termenilor, condițiilor și specificațiilor din documentele de atribuire, fără abateri esențiale sau cu abateri neînsemnate, erori sau omiteri ce pot fi înlăturate fără a afecta esența ei, se consideră conformă.

84. Autoritatea contractantă descalifică ofertantul care depune documente ce conțin informații false, cu scopul calificării, sau derutează ori face reprezentări neadevărate pentru a demonstra corespunderea sa cerințelor de calificare. În cazul în care acest lucru este dovedit, autoritatea contractantă declară ofertantul respectiv ca fiind neeligibil pentru participarea ulterioară în contractele de achiziții publice, în urma includerii lui în Lista de interdicție a operatorilor economici.

85. Autoritatea contractantă solicită ofertanților să demonstreze împlinirea de a încheia contractele de achiziții publice și componența fondatorilor, asociațiilor, acționarilor, administratorilor și a beneficiarilor efectivi.

86. Ofertantul/ofertantul asociat desemnat câștigător este obligat de a completa și prezenta declarația cu privire la beneficiarii efectivi în conformitate cu Ordinul ministrului finanțelor nr. 145/2020 cu privire la aprobarea Declarației privind confirmarea identității beneficiarilor efectivi și neîncadrarea acestora în situația condamnării pentru participarea la activități ale unei organizații sau grupări criminale, pentru corupție, fraudă și/sau spălare de bani.

Secțiunea a 6-a

Atribuirea contractului

87. Autoritatea contractantă anulează procedura de atribuire a contractului de achiziție publică conform art. 71 din Legea nr. 131/2015 privind achizițiile publice.

88. Decizia de anulare nu creează vreo obligație a autorității contractante față de ofertanți, cu excepția returnării garanției pentru ofertă. Decizia de anulare a procedurii de atribuire se expediază Agenției Achiziții Publice nu mai târziu de data informării despre rezultatele procedurii de atribuire prevăzută la art. 31 alin. (1) al Legii nr. 131/2015 privind achizițiile publice.

89. În cazul în care se anulează aplicarea procedurii pentru atribuirea contractului de achiziție publică, autoritatea contractantă are obligația de a comunica în scris tuturor participanților la procedura de achiziție publică, în cel mult 3 zile de la data anulării procedurii, atât încetarea obligațiilor pe care aceștia și le-au creat prin depunerea de oferte, cât și motivul anulării.

90. Darea de seamă privind anularea procedurii de achiziție publică este întocmită de către autoritatea contractantă și este publicată în Buletinul achizițiilor publice nu mai târziu de data emiterii deciziei de anulare a procedurii de achiziție publică.

91. La momentul încheierii contractului, dar nu mai târziu de data expirării garanției pentru ofertă, după caz, ofertantul câștigător prezintă garanția de bună execuție, în conformitate cu cerințele stipulate în art. 68 al Legii nr. 131/2015 privind achizițiile publice.

92. Garanția de bună execuție a contractului, dacă părțile agreează, se constituie din:

1) rețineri succesive din plata cuvenită pentru facturile fiscale înaintate, cu efectuarea transferului sumei respective pe un cont special deschis de către operatorul economic, pus la dispoziția autorității contractante, la o bancă licențiată, agreată de ambele părți;

2) rețineri succesive directe din plata cuvenită pentru facturile fiscale înaintate;

3) transfer pe contul autorității contractante;

4) formă de garanție bancară de la o instituție licențiată, (anexa nr.10).

93. Refuzul ofertantului câștigător de a depune garanția de bună execuție sau de a semna contractul constituie motiv pentru anularea atribuirii contractului și reținerii garanției pentru ofertă. În acest caz, autoritatea contractantă poate atribui contractul următorului ofertant cu oferta cea mai bine clasată, a cărei ofertă este conformă cerințelor și care este apreciată de către autoritatea contractantă a fi calificată în executarea contractului. Totodată, autoritatea contractantă este în drept să respingă toate celelalte oferte.

94. La expirarea perioadei de așteptare sau, după caz, după soluționarea oricăror contestații, sau monitorizării conformității desfășurării procedurilor de achiziții publice de către Agenția Achiziții Publice, autoritatea contractantă încheie contractul de achiziții publice, în conformitate cu termenii și condițiile indicate în documentația de atribuire.

95. La data încheierii contractului de achiziție publică de bunuri/servicii se interzice modificarea unor elemente ale ofertei câștigătoare, impunerea de noi cerințe ofertantului câștigător sau implicarea oricărui alt ofertant decât cel care a prezentat oferta cea mai avantajoasă.

96. Contractul pentru care sursele financiare se alocă din bugetul de stat/bugetul local se înregistrează obligatoriu la una din trezoreriile regionale ale Ministerului Finanțelor și intră în vigoare la data înregistrării sau la o altă dată ulterioară prevăzută de acesta după înregistrare la una din trezoreriile regionale ale Ministerului Finanțelor.

97. Autoritatea contractantă utilizează contractul - model (anexa nr. 24) din prezenta documentație-standard, inclusiv pentru contracte subsecvente încheiate conform acordului-cadru (anexa nr. 26), pentru contracte de valoare mică, pentru contractele în urma desfășurării procedurii prin cererea ofertelor de prețuri, la fel și pentru contractele în urma desfășurării

procedurilor negociate. Contractul poate fi încheiat între una sau mai multe autorități contractante și unul sau mai mulți operatori economici, care are ca obiect livrarea/prestarea bunurilor/serviciilor.

98. Contractul este compus din două părți: Partea I cea generală care este obligatorie, și care nu se modifică, doar cu excepția contractelor de achiziții publice ce nu cad sub incidența Legii nr. 131/2015 privind achizițiile publice și Partea II ceea ce ține de condițiile speciale al contractului care se completează doar la necesitate, unde autoritatea contractantă are dreptul de a stabili condiții/cerințe speciale în dependență de obiectul achiziției, de complexitatea procedurii, atât și de a stabili condițiile achitării (în special la achiziționarea combustibilului, energiei electrice, gaze, apa și canalizare, salubritate, servicii de comunicații electronice, etc.), atât și de a stabili condițiile achitării în avans. În cazul achizițiilor serviciilor din domeniul energetic și de alimentare cu apă și de canalizare, contractul de achiziții publice conține clauzele obligatorii stabilite prin legile sectoriale și actele normative de reglementare aprobate de către ANRE. Totodată, prevederile obligatorii stabilite prin deciziile acestora, care nu se regăsesc în partea I cea generală al contractului, se indică în partea II ce ține de condițiile speciale al contractului.

99. Termenii de asumare a angajamentelor în contractele de achiziții publice de către autoritățile/instituțiile bugetare se stabilesc în conformitate cu prevederile art. 66 din Legea nr. 181/2015 finanțelor publice și responsabilității bugetar-fiscale.

100. În cazul serviciilor de audit, autoritatea contractantă indică în partea II ce ține de condițiile speciale al contractului drepturile/obligatiile Beneficiarului și drepturile/obligatiile Prestatorului, în conformitate cu prevederile Ordinului ministrului finanțelor nr. 160/2020 cu privire la aprobarea Regulamentului privind activitatea de audit intern pe bază de contract în sectorul public.

101. Nu se acceptă în cadrul achizițiilor publice proiectele contractelor ce deviază de la anexa nr. 24, întocmite de prestator/furnizor cu excepția cazurilor când serviciile sunt prestate în afara țării și sunt încheiate conform cadrului juridic local (de exemplu: serviciile de instruire, servicii hoteliere, etc.).

102. Orice operator economic care consideră că, în cadrul procedurilor de achiziție, autoritatea contractantă, prin decizia emisă sau prin procedura de achiziție aplicată cu încălcarea legii, a lezat un drept al său recunoscut de lege, în urma cărui fapt el a suportat sau poate suporta prejudicii, are dreptul să conteste decizia sau procedura aplicată de autoritatea contractantă, în modul stabilit de Legea nr. 131/2015 privind achizițiile publice.

103. Contestațiile se depun direct la Agenția Națională pentru Soluționare a Contestațiilor. Toate contestațiile se depun, se examinează și se soluționează în modul stabilit de Legea nr. 131/2015 privind achizițiile publice.

104. Operatorul economic, conform art. 83 al Legii nr. 131/2015 privind achizițiile publice, în termen de până la 5 zile, sau 10 zile de la data la care a aflat despre circumstanțele ce au servit drept temei pentru contestație, are dreptul să depună la Agenția Națională pentru Soluționarea Contestațiilor o contestație argumentată a acțiunilor, a deciziei ori a procedurii aplicate de autoritatea contractantă.

105. Contestațiile privind anunțurile de participare la licitație și documentația de atribuire se depun în termenele indicate la pct. 104, însă nu mai târziu de deschiderea ofertelor de către autoritatea contractantă.

106. Fiecare ofertant care participă, în mod individual sau ca asociat, la procedura de atribuire a contractului de achiziție publică de bunuri/servicii are obligația să prezinte anexele prevăzute în prezenta documentație, completate în mod corespunzător și semnate de persoanele autorizate, conform cerințelor stabilite în anexa nr.2.

ANUNȚ DE PARTICIPARE INCLUSIV PENTRU PROCEDURILE DE PRESELECȚIE/PROCEDURILE NEGOCIATE

privind achiziționarea: [Echipamente de rețea de tip Next Generation Firewall \(NGFW\)](#)

prin procedura de achiziție *Cererea ofertelor de preț*

**Procedura a fost inclusă în planul de achiziții publice a autorității contractante*

(Da/Nu): Da

Link-ul către planul de achiziții publice publicat:

<https://cnas.gov.md/ro/transparenta/achizitii-publice/planuri-de-achizitii-publice>

1. Denumirea autorității contractante: *Casa Națională de Asigurări Sociale*
2. IDNO: *1004600030235*
3. Adresa: *mun. Chișinău, str. Gh. Tudor, 3*
4. Numărul de telefon/fax: *022-257-681; 022-257-840; 022-257-752 .*
5. Adresa de e-mail și pagina web oficială ale autorității contractante:
achizitiicnas@cnas.gov.md , www.cnas.gov.md ;
6. Adresa de e-mail sau de internet de la care se va putea obține accesul la
documentația de atribuire: *documentația de atribuire sunt anexate în cadrul
procedurii în M-Tender SIA RSAP.*
7. Tipul autorității contractante și obiectul principal de activitate (dacă este cazul,
mențiunea că autoritatea contractantă este o autoritate centrală de achiziție sau că
achiziția implică o altă formă de achiziție comună): *Nu se aplică*
8. Cumpărătorul invită operatorii economici interesați, care îi pot satisface
necesitățile, să participe la procedura de achiziție privind livrarea următoarelor
bunuri:

Codul CPV: 32420000-3 echipamente de rețea

Specificația tehnică

Denumire bunurilor solicitate	Specificarea tehnică deplină solicitată, Standarde de referință	Cantita tea	Valoare a estimat ă fără TVA lei MLD	Pasul minim de licitare (electr onică) lei MLD
-------------------------------------	--	----------------	---	---

1.	<u>Echipamente de rețea de tip Next Generation Firewall (NGFW)</u> <u>Cerințe tehnice</u> 1. Protecția rețelei cu controlul stării sesiunilor; 2. Recunoașterea și blocarea aplicațiilor de rețea la nivelul 7 al modelului OSI în funcție de traficul care trece prin firewall, inclusiv individual pentru toate aplicațiile care folosesc porturi comune, inclusiv 80 și 443, precum și pentru aplicațiile care utilizează porturi TCP/UDP dinamice; 3. Firewall-ul NGFW propus trebuie să fie certificat minim conform standardelor ISO 27001, ISO 27017, ISO 27018, ISO 27701, Germany C5, Common Criteria, FIPS 140-2, CMVP. 4. Firewall-ul NGFW propus nu trebuie să necesite o repornire pentru a verifica și instala actualizările de securitate. 5. Firewall-ul NGFW propus trebuie să poată identifica aplicațiile indiferent de portul utilizat, criptarea SSL/SSH sau metodele de ocolire folosite. 6. Firewall-ul NGFW propus trebuie să clasifice aplicațiile neidentificate pentru gestionarea politicii, analiza criminalistică a amenințărilor sau dezvoltarea tehnologiilor de identificare a aplicațiilor. 7. Firewall-ul NGFW propus trebuie să fie o soluție dezvoltată inițial pentru asigurarea securității (nu un management de aplicații cu un firewall de bază care verifică starea). 8. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas. 9. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas. 10. Firewall-ul NGFW propus trebuie să poată să delimiteze diferite părți ale unei aplicații, cum ar fi permiterea chat-ului pe Facebook, dar blocarea posibilității de a trimite fișiere. 11. Firewall-ul NGFW propus trebuie să controleze accesul și să aplice politici pentru site-uri web și aplicații, inclusiv pentru aplicațiile SaaS. 12. Firewall-ul NGFW propus trebuie să utilizeze un sistem de operare unificat în toate formatele. 13. Firewall-ul NGFW propus trebuie să sprijine crearea politicii de securitate pentru prevenirea furtului de credențiale. 14. Firewall-ul NGFW propus trebuie să sprijine aplicarea autentificării multi-factor pentru aplicațiile interne. 15. Firewall-ul NGFW propus trebuie să permită vizibilitatea și controlul aplicațiilor care folosesc porturi non-standard, într-o politică unică de securitate. 16. Firewall-ul NGFW propus trebuie să poată oferi algoritmi de învățare automată pentru protecție avansată direct din NGFW, fără a necesita conexiuni externe.	10 bucăți	387 000,00	3 800,00
----	---	--------------	------------	----------

	17. Recunoașterea în traficul inspectat la Layer-7 al modelului OSI a semnăturilor stocate pe MFE pentru următoarele categorii de aplicații: 17.1 . Aplicații corporative: 17.1.1. Servicii de autentificare, inclusiv Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS; 17.1.2. Sisteme de gestionare a bazelor de date (SGBD), inclusiv Microsoft SQL, Oracle, DB2, Postgres, Sybase; 17.1.3. Servicii de fișiere, inclusiv Microsoft SMB. 17.1.4. ERP, CRM, inclusiv SAP, 1C; 17.1.5. Sisteme de management al documentelor electronice și schimb de mesaje, inclusiv EMC Documentum, Microsoft SharePoint, Exchange, Lync, Office 365, Google Docs, Lotus; 17.1.6. Protocoale de schimb de e-mail: SMTP, POP3, IMAP; 17.1.7. Protocoale VoIP și conferințe audio-video, inclusiv SIP, H.323, H.245, H.225, Webex; 17.1.8. Servicii de actualizare software, inclusiv Microsoft Update, software antivirus (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple; 17.1.9. Servicii de backup, inclusiv Symantec Backup Exec; 17.1.10.Servicii de virtualizare și acces la terminale, inclusiv VMware, Citrix, Microsoft RDP; 17.1.11.Alte protocoale și tehnologii utilizate pentru crearea aplicațiilor distribuite, inclusiv CORBA, SOAP; 17.1.12.Protocoale de acces de la distanță, inclusiv Telnet, SSH, VNC, Radmin; 17.1.13.Protocoale de rețea, inclusiv protocoale de rutare dinamică și SSL, IPsec VPN; 17.2. Aplicații Internet: 17.2.1. E-mail, inclusiv Gmail, Yandex.Mail, Mail.ru, Hotmail; 17.2.2. Rețele sociale, inclusiv Facebook, Google+, LinkedIn, ВКонтакте, Odnoklassniki, „Moy Mir”; 17.2.3. Servicii de mesagerie instantanee, inclusiv Jabber, IRC, MSN, servicii similare în cadrul rețelelor sociale enumerate mai sus; 17.2.4. Servicii de conferință audio-video 17.2.5. Servicii de schimb de fișiere prin HTTP(S) și peer-to-peer, inclusiv Dropbox, BitTorrent, eMule, Google Drive, Yandex Disk, Gnutella, Boxnet, WebDav; 17.2.6. Streaming audio-video (indiferent de site-ul web), inclusiv YouTube, Vimeo, audio și video prin HTTP; 17.2.7. Servicii de publicare a desktop-ului și oferirea de acces de la distanță, inclusiv TeamViewer, LogMeIn; 17.2.8. Proxy externe și anonimizatoare, inclusiv Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy; 17.2.9. Servicii de construire a VPN-urilor private și tuneluri deasupra altor aplicații, inclusiv FreeNet, Open-VPN, VTun, RDP-to-TCP, TCP-over-DNS; 18. Oferirea de instrumente integrate în MFE pentru crearea semnăturilor proprii de aplicații bazate pe expresii regulate folosind decodare pentru HTTP(S), FTP, SMB, SMTP, RPC și altele, precum și pe mască pentru conținutul pachetelor TCP/UDP; 19. Recunoașterea aplicațiilor transmise prin protocolul HTTP/2; 20. Recunoașterea aplicațiilor de rețea prin traficul criptat SSL			
--	---	--	--	--

	(suport pentru chei RSA de până la 2048 de biți) și SSHv2 care trece prin firewall (decriptarea SSL, SSHv2) – atât pentru conexiunile intrante, cât și pentru cele ieșite, transparent pentru utilizatori în domeniu, cu posibilitatea de a controla funcțiile individuale ale aplicațiilor, inclusiv trimiterea de mesaje pe rețelele sociale, schimbul de fișiere, streaming audio și video; 21. Inspecția tunelurilor: 21.1. Generic Routing Encapsulation (GRE) (RFC 2784); 21.2. Trafic IPsec necriptat [NULL Encryption Algorithm pentru IPsec (RFC 2410)]; 21.3. Mod de transport AH IPsec. 22. Recunoașterea secvențială a diferitelor aplicații utilizate într-o singură sesiune; 23. Recunoașterea utilizatorilor care folosesc aplicații de rețea prin integrarea cu serviciile corporative de autentificare a utilizatorilor, cum ar fi Microsoft Active Directory, Microsoft Exchange, Novell eDirectory, LDAP, Citrix; posibilitatea integrării cu alte servicii de autentificare (de exemplu, controlerele de rețea wireless) printr-o API XML deschisă; posibilitatea de a utiliza autentificarea forțată a utilizatorilor folosind o pagină WEB – „Captive portal”; suport pentru Kerberos, Tacacs+, SAML v.2, suport pentru roaming-ul L3 al utilizatorilor prin sondaje WMI și NetBios; 24. Inspecția în timp real a conținutului traficului transmis prin firewall pe baza semnăturilor și comportamentului, protecția împotriva vulnerabilităților, atacurilor de rețea și a malware-ului, recunoașterea tipurilor de fișiere pe baza semnăturilor acestora, detectarea virusilor transmiși prin web, e-mail, FTP, SMB, spyware, viermi de rețea, blocarea transmiterii unor conținuturi specifice folosind expresii regulate, inclusiv pentru aplicațiile care utilizează criptare SSL și SSHv2; 25. Crearea de reguli pentru traficul care trece prin firewall într-o politică unificată de securitate, utilizând următorii parametri pentru fiecare conexiune: 25.1. Adresa IP a expeditorului, 25.2. Adresa IP a destinatarului, 25.3. Serviciile L4 utilizate: porturi pentru protocoalele TCP și UDP, 25.4. Numele utilizatorilor sau grupurilor de utilizatori din Active Directory, 25.5. Aplicațiile la nivelul 7 al modelului OSI, 25.6. URL categorii. 26. Crearea de reguli într-o politică unificată de securitate, utilizând ca parametri informațiile despre adresele IP ale expeditorului, destinatarului, serviciile utilizate (porturi TCP/UDP), numele utilizatorilor, grupurilor de utilizatori și aplicațiile utilizate de aceștia sau anumite categorii de aplicații. În politicile create, trebuie să existe posibilitatea implementării următoarelor acțiuni: • Permisivitate sau interdicție; • Permisivitatea unui anumit aplicații sau categorii de aplicații de a utiliza doar porturi TCP/UDP standard sau strict definite. Aceste porturi nu trebuie să fie folosite de alte aplicații fără o politică care să permită explicit astfel de			
--	---	--	--	--

	interacțiuni; • Permisiiune, dar cu scanare pentru viruși și alte amenințări; • Permisiiune sau interdicție pe bază de orar, utilizator sau grup de utilizatori; • Decriptare și verificare. Dacă nu s-a putut decripta (în cazul unui algoritm criptografic nestandard, certificat expirat etc.) – interzicere; • Ne-decriptarea anumitor categorii de URL și site-uri web de încredere; • Aplicarea marcajului DSCP și limitarea traficului folosind politici QoS bazate pe aplicații, adrese IP, utilizatori și grupuri de utilizatori; • Implementarea hardware a QoS pentru traficul real-time, identificat la nivelul aplicațiilor; • Aplicarea redirectionării traficului pe bază de politici (Policy Based Forwarding); • Permisiiunea anumitor funcții ale aplicației; • Oricare combinație dintre acțiunile de mai sus. 27. Protecție antivirus, protecție împotriva software-ului spyware, protecție împotriva vulnerabilităților și atacurilor de rețea (sistem de detecție și prevenire a intruziunilor), filtrare URL utilizând o bază dinamică de reputație, care susține categorizarea diferitelor secțiuni ale aceluiași site web, inclusiv susținerea categoriilor pentru site-uri web în limba rusă, blocarea transferului de fișiere pe baza tipurilor definite de semnături; 28. Posibilitatea de a verifica suplimentar traficul pentru amenințări necunoscute prin analiza acestuia utilizând tehnologia învățării automate prin servicii cloud; 29. Detectarea și filtrarea solicitărilor către resursele din rețea în funcție de categoria acestora, de exemplu, site-uri malware, rețele sociale, resurse publicitare etc.; 30. Suport pentru acțiuni: permisiune, notificare, blocare, solicitarea confirmării utilizatorului, solicitarea parolei utilizatorului; 31. Filtrarea URL trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 32. Analiza SNI în TLS Hello simultan cu URL-ul în cererea HTTP pentru a contracara tehnicile de ocolire de tip SNIcat; 33. Analiza cererilor DNS suspecte, domeniilor DGA și localizarea stațiilor infectate utilizând tehnologia DNS sinkhole (modificarea răspunsului serverului DNS); 34. Detectarea tehnicilor de ocolire a protecției prin cereri DNS care încearcă să folosească domenii generate automat (DGA), inclusiv analiza frecvenței n-gramelor, analiza entropiei, frecvența cererilor, tunelarea în DNS, canale de transfer de date prin cereri DNS, inclusiv tuneluri DNS ultra-lente; 35. Blocarea domeniilor DGA, domeniilor DGA create pe baza unui dicționar, tehnici de ocolire DNS-rebinding, FastFlux, interogări către înregistrări DNS suspendate, atacuri NSNX, atacuri cu domenii recent înregistrate; 36. Analiza cererilor DNS suspecte trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 37. Protecție împotriva tehnicilor de evitare (evasions), de			
--	---	--	--	--

	exemplu MPTCP; 38. Oferirea unui serviciu de scanare a fișierelor potențial dăunătoare necunoscute în sandbox cu sisteme de operare Microsoft Windows, Linux prin metoda de emulare a rulării și vizualizare a documentelor; 39. Sandbox-ul trebuie să verifice fișierele executabile suspecte (inclusiv EXE, DLL, SCR, BAT, etc.), fișiere ELF, documente în formatele PDF, MS Office 2007, 2010, 2016 și mai sus, Java și Flash, Android APK, Mach-O, DMG și PKG, arhive RAR, ZIP, 7Zip; 40. Firewall-ul trebuie să trimită spre verificare în sandbox fișierele suspecte transmise prin aplicațiile HTTP, SMTP, POP3, IMAP, SMB, FTP, precum și implementările acestora prin SSL, dacă există; 41. Sandbox-ul trebuie să genereze și să trimită către firewall un raport despre verificarea fișierului; 42. Sandbox-ul trebuie să genereze semnături pentru blocarea atacurilor de tip zero-day pentru utilizarea pe toate firewall-urile companiei în aplicațiile enumerate, în decurs de 5 minute de la primirea fișierului pentru verificare; 43. Firewall-ul trebuie să primească semnăturile fișierelor din sandbox și să aibă un motor de blocare bazat pe noile semnături obținute de la sandbox-ul cloud sau local; 44. Sandbox-ul furnizorului cloud trebuie să aibă posibilitatea de a schimba semnături între toți clienții furnizorului; 45. Firewall-ul trebuie să primească din sandbox indicatori de compromitere: IP, URL, DNS, care sunt utilizate de codul malițios și să blocheze conexiunile pe baza listei de indicatori malițioși. 46. Sandbox-ul trebuie să verifice linkurile HTTP:// și HTTPS:// din e-mailuri prin protocoalele SMTP/POP3. 47. Sandbox-ul trebuie să verifice fișierele din aplicațiile criptate SSL, cel puțin în protocolul HTTPS. 48. Suport obligatoriu pentru învățarea automată în timpul inspecției amenințărilor de tip zero-day pentru a reduce întârzierea în inspecția fișierelor suspecte; 49. Sandbox-ul trebuie să asigure analiza comportamentului fișierelor și linkurilor suspecte în cloud privat sau extern (sandbox), să detecteze noi malware și să genereze automat semnături antivirus în decurs de 5 minute și să actualizeze baza de reputație URL în decurs de 30 de minute, care se vor instala pe toate dispozitivele Clientului cu abonamentele corespunzătoare; 50. Posibilitatea integrării cu subsistemul de detectare a amenințărilor zero-day, implementat pe un dispozitiv hardware dedicat aceluiași furnizor, plasat pe obiectul central al Clientului (cloud privat), care permite generarea automată a semnăturii antivirus local, pe dispozitivul hardware dedicat în centrul de date (DC) al Clientului în decurs de 5 minute; 51. Sandbox-ul local dedicat trebuie să aibă un API pentru primirea fișierelor spre verificare atât de la firewall-uri, cât și de la servicii terțe; 52. Sandbox-ul trebuie să genereze rapoarte despre verificările efectuate și să permită vizualizarea acestora în format PDF; 53. Sandbox-ul cloud trebuie să utilizeze tehnologia Bare Metal Analysis fără a utiliza emularea sistemului de			
--	--	--	--	--

	operare; 54. Firewall-ul trebuie să aibă capacitatea de a trimite fișiere diferite în sandbox-uri diferite, de exemplu, fișierele EXE în sandbox-ul cloud, iar fișierele DOC în sandbox-ul local; 55. Sandbox-ul cloud trebuie să accepte fișiere PE pentru verificare, chiar și în absența unui abonament; 56. Suport pentru următorii furnizori de autentificare multi-factor (Multi-Factor Authentication - MFA) (direct, fără utilizarea produselor intermediare): Duo, • Okta, • RSA SecureID, • PingID; 57. Protecție împotriva furtului de loginuri și parole ale utilizatorilor prin integrarea cu Active Directory (AD), monitorizarea transiterii conturilor de utilizator către zone de securitate neîncredere, autentificarea forțată a utilizatorilor prin autentificare cu doi factori (MFA); 58. Funcționalitate de control granular al accesului utilizatorilor de la distanță în mediul de lucru corporativ, cu posibilitatea de verificare a existenței anumitor software-uri pe stația de lucru a utilizatorului și accesul prin dispozitive mobile; 59. Funcționalitate de protecție împotriva atacurilor DoS; 60. Posibilitatea de a activa 100% din semnăturile IPS, antivirus, filtrarea URL-urilor, controlul aplicațiilor și Threat Intelligence fără a degrada performanța; 61. Funcționalitate de blocare a scanării porturilor ICMP/TCP/UDP; 62. Detectarea obiectelor din fișierele transmise prin rețea care conțin informații importante și blocarea transiterii acestor fișiere; 63. Detectarea prezenței datelor filtrabile în fișierele transmise prin rețea, incluzând, dar fără a se limita la: Adobe PDF, HTML, Microsoft Office (Excel, Word, PowerPoint). Rich Text Format; 64. Prezența șabloanelor de date preconfigurate, cum ar fi numerele de carduri de credit. 65. Suport pentru crearea de șabloane proprii de date pe baza expresiilor regulate. 66. Posibilitatea de integrare cu subsistemul de management centralizat, logare, raportare și actualizare a software-ului pentru firewall-uri de același furnizor. 67. Cerințe pentru sistemul de management centralizat: • Funcționalități avansate de vizualizare a activității aplicațiilor rețelei, amenințărilor rețelei detectate și blocate, utilizarea aplicațiilor de către utilizatori. Permite filtrarea informațiilor pe aplicații, amenințări, utilizatori, adrese IP, porturi TCP/UDP, zone de securitate, tipuri de amenințări etc.; • Corelarea automată a jurnalelor de diferite tipuri, generate în cadrul aceleași sesiuni (filtrarea traficului prin firewall, protecția împotriva amenințărilor, controlul transferului de fișiere, filtrarea URL); • Posibilitatea de corelare automată a evenimentelor de securitate folosind obiecte de corelare actualizabile care folosesc informații de la protecția antivirus, protecția			
--	--	--	--	--

	împotriva software-ului spyware, protecția împotriva vulnerabilităților și atacurilor, amenințările de tip zero-day; • Funcționalități de generare automată a rapoartelor și de generare a rapoartelor pe bază de program, cu opțiuni de personalizare manuală a rapoartelor. Rapoartele trebuie să fie vizibile prin interfața grafică (GUI) și să poată fi exportate în formate PDF și CSV. • Posibilitatea de a configura funcționalitățile SD-WAN prin consola de management centralizat. • Sistemul trebuie să poată exporta logurile către soluții externe prin syslog, utilizând formate standardizate precum CEF sau LEEF; • Trebuie să existe mecanisme de inițializare automată pentru echipamente noi, inclusiv în locații la distanță, fără intervenție manuală; • Trebuie să fie posibilă actualizarea centralizată a software-ului pentru echipamentele administrate, într-un mod simplificat; • Soluția trebuie să ofere interfețe moderne de integrare (REST API) compatibile cu XML și JSON, pentru interoperabilitate cu alte sisteme. • Fiecare administrator trebuie să poată face modificări izolate, cu salvare separată, pentru a evita suprascrierea neintenționată; • Sistemul trebuie să permită definirea de roluri și permisiuni personalizate pentru utilizatori, cu acces diferențiat la funcționalități. • Platforma trebuie să permită organizarea echipamentelor și configurațiilor prin grupuri, ierarhii și etichete; • Sistemul trebuie să suporte funcționare în mod redundant (high availability) și echilibrare a sarcinii (load balancing); 68. Posibilitatea de a detecta și analiza traficul dispozitivelor IoT folosind algoritmi de învățare automată. 69. Funcționalitatea de a trimite traficul SSL decriptat către dispozitive externe. 70. Funcționalitatea de a captura traficul de la dispozitive externe și de a-l cripta într-un tunel SSL pentru transmiterea prin Internet. 71. Prezența unui raport separat pentru aplicațiile de tip SaaS. 72. Funcționalitatea IPsec VPN. 73. Integrarea cu sistemele externe SIEM/SIM prin protocolul Syslog, cu configurare flexibilă a formatului jurnalelor. 74. Suport pentru rutare statică și protocoale de rutare dinamică BGP, OSPF, RIP. 75. Suport pentru diverse moduri de lucru ale interfețelor rețelei (monitorizare trafic mirroring, mod transparent, Layer 2 și Layer 3). 76. Suport pentru IPv6, inclusiv identificarea aplicațiilor și utilizatorilor. 77. Suport pentru multicast, incluzând PIM-SM, PIM-SSM, IGMP v1, v2, v3. 78. Suport pentru rutarea între VLAN-uri. 79. Suport pentru NAT, DHCP și DHCP relay. 80. Suport pentru etichetarea cadrelor prin 802.1Q (minim 4094 VLAN-uri). 81. Suport pentru agregarea interfețelor prin 802.3ad (suport LACP).			
--	--	--	--	--

	82. Suport pentru pachete mari (Jumbo frames). 83. Managementul rolurilor administratorilor locali: • Posibilitatea de a restricționa vizualizarea și gestionarea la nivelul dispozitivului și al sistemelor virtuale (contexte); • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la orice secțiune a interfeței web; • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la CLI-ul firewall-ului. 84. Firewall-ul hardware trebuie să dispună de o platformă hardware specializată, care să permită administrarea dispozitivului fără întreruperi, chiar și în condiții de încărcare maximă. Trebuie să fie asigurate resurse de procesare dedicate, separate pentru analiza traficului monitorizat și pentru activitățile de management. Administrarea fiecărui dispozitiv în parte trebuie să se realizeze prin protocoalele HTTPS și SSH, fără a necesita instalarea vreunui software suplimentar de administrare pe stația de lucru a administratorului. Interfața de administrare a firewall-urilor (web și CLI) trebuie să fie unificată cu subsistemul de management centralizat, jurnalizare, raportare și actualizare a software-ului. Cerințe de performanță ale firewall-ului: Performance: • Threat prevention throughput 1.2 Gbps; • IPsec VPN throughput 800 Mbps; • Connections per second 1100; • Firewall throughput 1.4 Gbps; Policies: • Security rules min 500; • Security rule schedules min 256; • NAT rules min 400; • Tunnel content inspection rules 100; • SD-WAN rules min 100; • Policy based forwarding rules min 100; • DoS protection rules min 100. Security Zones: • security zones 25. Security Profiles: • Security profiles min 75. URL Filtering: • Total entries for allow list, block list and custom categories 25,000; Interfaces: • I/O: 1G RJ45 (7); • Management I/O: 10/100/1000 out-of-band management port (1), RJ45 console port (1), USB port (1). Storage Capacity: • 128 GB			
--	--	--	--	--

	Virtual Routers: • Virtual routers 3. Routing: • IPv4 forwarding table size min 5,000; • IPv6 forwarding table size min 2500; • System total forwarding table size min 5,000; L2 Forwarding: • ARP table size per device 1500; • IPv6 neighbor table size 1500; • MAC table size per device 1500; Address Assignment: • DHCP servers 3; • DHCP relays 500; • IPSec VPN: • Suport Site to site over gre IPSec tunnels • SD-WAN IPsec tunnels 85. Alte cerințe obligatorii: - Garanție, Mentenanța și Suport HW+SW incluse – 12 luni; - Producătorul trebuie să ofere suport prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului; - Ofertantul va indica în ofertă costul serviciilor pentru efectuarea instalării și configurării a echipamentului oferat, va asigura integrarea echipamentului oferat cu dispozitivele existente pe baza platformei existente în cadrul instituției prin realizarea configurărilor necesare, cu setarea tuturor parametrilor aplicabili în corespundere cu cerințele înaintate pe infrastructura Beneficiarului. - Prezentarea a certificatelor a minim 1 specialist pe produsul oferat din partea ofertantului (fără asociere cu o altă companie); - Ofertantul va prezenta copia Certificatului ISO 27001:2018, în domeniul serviciilor privind asigurarea securității informației, design-ul acestuia, implementarea, monitorizarea și managementul infrastructurii IT - Ofertantul va prezenta Certificatului ISO 9001:2015, pentru Servicii de comercializare și implementare suport tehnic în garanție și post garanție pentru sisteme informaționale, echipamente hardware și software și Servicii privind asigurarea securității informației, designul, implementarea, monitorizarea și managementul infrastructurii IT și de Securitate – certificat confirmat cu aplicarea semnăturii electronice; - Ofertantul va prezenta Autorizarea de la producător pentru licitația la care participa; - Ofertantul va avea minim o persoană certificată în calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013; - Referințe de vânzare NGFW – minim 3 contracte; - Termen de livrare: maxim până la 90 zile de la data intrării în vigoare a contractului			
Valoarea estimativă	387 000,00			

Cerințe suplimentare se vor include ca parte componentă a contractului:

1. Echipamentul propus trebuie să fie furnizat de producători recunoscuți mondiali (BRAND NAME).
2. Furnizorul va asigura instalarea și configurarea echipamentului prin specialiștii certificați menționați în ofertă, în ferestre de mentenanță agreate, fără întreruperea serviciilor critice.
3. Garanția echipamentelor livrate cade în răspunderea vânzătorului pe toată perioada de garanție definită în ofertă.
4. În cazul apariției unor defecțiuni în perioada de garanție, furnizorul are obligația de a efectua reparațiile necesare sau de a asigura înlocuirea elementelor defecte cu piese de rezervă conforme, pe propria cheltuială. Deservirea în cazul unor neajunsuri sau defectări tehnice a utilajului are loc conform programului de lucru de către furnizor la Aparatul Central CNAS. Recepționarea și livrarea utilajului reparat în baza garanției se efectuează la sediul Aparatului Central CNAS.
5. Bunurile vor fi livrate cu transportul Vânzătorului și descărcate în depozitul aparatului central CNAS mun. Chișinău, str. Gheorghe Tudor 3.
6. Bunurile livrate urmează să fie însoțite de certificatul de origine și certificatul de atestare a calității echipamentului.
7. Bunurile livrate trebuie să fie noi, nefolosite și ne-reconstruite (non-refurbished) și să nu fie fabricate cu mai mult de 12 luni înainte de data livrării.
9. **În cazul procedurilor de preselecție se indică numărul minim al candidaților și, dacă este cazul, numărul maxim al acestora.** Nu se aplică
10. **În cazul în care contractul este împărțit pe loturi un operator economic poate depune oferta (se va selecta):**
 - 1). Pentru fiecare lot în parte
11. **Admiterea sau interzicerea ofertelor alternative:** Nu se admite
12. **Termenii și condițiile de livrare/prestare/executare solicitați:** Timp de 90 zile din data înaintării comunicării către Vânzător privind transmiterea dării de seamă la Agenția Achiziții Publice, cu livrare și descărcare a bunurilor la depozitul CNAS din str. Gheorghe Tudor nr. 3 mun. Chișinău, cu recepționarea de către persoana responsabilă desemnată din cadrul CNAS.
13. **Termenul de valabilitate a contractului :** 31.12.2026
14. **Contract de achiziție rezervat atelierelor protejate sau că acesta poate fi executat numai în cadrul unor programe de angajare protejată (după caz):** Nu se aplică
15. **Prestarea serviciului este rezervată unei anumite profesii în temeiul unor acte cu putere de lege sau al unor acte administrative (după caz):** Nu se aplică
16. **Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora și a criteriilor de selecție; nivelul minim (nivelurile minime) al (ale) cerințelor eventual impuse; se menționează informațiile solicitate (DUAЕ, documentație):**

Nr. d/o	Criteriile de calificare și de selecție (Descrierea criteriului/cerinței)	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativitatea
1	Prezentarea Cererii de participare conform Anexei nr.7 din Ordinul MF 115/2021.	Cerere de participare confirmată prin semnătura electronică	Obligativiu
2	Prezentarea Declarației privind valabilitatea ofertei conform Anexei nr.8 din Ordinul MF 115/2021	Declarația privind valabilitatea ofertei confirmată prin semnătura electronică	Obligativiu
3	Prezentarea Specificații de preț conform Anexei nr.23 din Ordinul MF 115/2021	Specificații de preț, confirmat prin semnătura electronică	Obligativiu
4	Prezentarea Specificații tehnice conform Anexei nr.22 din Ordinul MF 115/2021	Specificații tehnice, confirmată prin semnătura electronică .	Obligativiu
5	Prezentarea Formularul standard al Documentului Unic de Achiziții European completat	Formularul standard al Documentului Unic de Achiziții European confirmat prin semnătura electronică	Obligativiu
6	Vor fi excluși operatorii economici care nu și-au îndeplinit obligațiile de plată a impozitelor, taxelor și contribuțiilor de asigurări sociale în conformitate cu prevederile legale în vigoare în Republica Moldova sau în țara în care este stabilit.	Accesarea informației privind îndeplinirea obligațiilor de plată a impozitelor, taxelor și contribuțiilor de asigurări sociale de către candidatul sau ofertantul la procedura de atribuire a contractului de achiziții publice se va efectua nemijlocit de către autoritatea contractantă prin accesarea de către autoritățile contractante de pe platforma de interoperabilitate (MConnect), precum și de pe Portalul guvernamental de date, accesând următorul link: https://date.gov.md/open/company-details ..	Obligativiu
7	Vor fi excluși operatorii economici care nu dispun de capacitatea de exercitare a activității profesionale	- operatorul economic participant la licitație trebuie să dețină un centru de deservire de garanție a bunurilor livrate sau contract cu un asemenea centru de deservire valabil la data deschiderii ofertei. - Producător de calculatoare trebuie să fie recunoscut mondial (BRAND NAME). - Ofertantul va prezenta copia Certificatului ISO 27001:2018, în domeniul serviciilor privind asigurarea securității informației, design-ul acestuia, implementarea, monitorizarea și managementul infrastructurii IT - Ofertantul va prezenta Certificatului ISO 9001:2015, pentru Servicii de comercializare și implementare suport tehnic în garanție și post garanție pentru sisteme informaționale, echipamente hardware și software și Servicii privind asigurarea securității informației, designul, implementarea, monitorizarea și managementul infrastructurii IT și de Securitate – certificat confirmat cu aplicarea semnăturii electronice; - Ofertantul va prezenta Autorizarea de la producător pentru licitația la care participa; - Prezentarea a certificatelor a minim 1	Obligativiu

		specialist pe produsul oferat din partea ofertantului (fără asociere cu o alta companie); - Ofertantul va avea minim o persoana certificata in calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013;	
8	Vor fi excluși operatorii economici care nu dispun de standarde de asigurare a calității	Declarație pe proprie răspundere referitor la - Garanția echipamentelor livrate cade în răspunderea vânzătorului pe toată perioada de garanție și constituie 12 luni. - Producătorul trebuie să ofere suport prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului - În caz de defecție a echipamentului furnizorul trebuie să asigure repararea elementelor defectate sau să dețină rezerve necesare pentru substituie lor în baza garanției. Deservirea în cazul unor neajunsuri sau defectări tehnice a utilajului are loc conform programului de lucru de către furnizor la Aparatul Central CNAS. Recepționarea și livrarea utilajului reparat în baza garanției se efectuează la sediul Aparatului Central CNAS. - Bunurile livrate urmează să nu fie mai vechi de un an de la data livrării și să fie noi (non refurbished).	Obligatori
9	Va fi exclus orice operator economic care nu deține numărul de înregistrare a producătorului în Lista producătorilor	Declarație pe propria răspundere privind numărul de înregistrare a producătorului de echipamente electrice și electronice în Lista producătorilor de produse supuse reglementărilor de responsabilitate extinsă a producătorilor (HG 212/2018) - confirmată prin semnătura electronică a Participantului	Obligatori
10	Va fi exclus din procedura de atribuire a contractului de achiziții publice orice ofertant sau candidat despre care are cunoștință că, în ultimii 5 ani, a fost condamnat, prin hotărârea definitivă a unei instanțe judecătorești, pentru participare la activități ale unei organizații sau grupări criminale, pentru corupție, pentru fraudă și/sau pentru spălare de bani, pentru infracțiuni de terorism sau infracțiuni legate de activități teroriste, finanțarea terorismului, exploatarea prin muncă a copiilor și alte forme de trafic de persoane.	La depunerea ofertei prin declararea în DUAE/la evaluare la solicitarea AC	Obligatori <i>Lipsa condamnării pe parcursul a ultimilor 5 ani.</i>
11	Va fi exclus orice operator economic care se află în proces de insolvență ca urmare a hotărârii judecătorești.	La depunerea ofertei prin declararea în DUAE	Obligatori <i>Nu se află în proces de</i>

			<i>insolvabilitate</i>
12	DECLARAȚIE privind confirmarea identității beneficiarilor efectivi și neîncadrarea acestora în situația condamnării pentru participarea la activități ale unei organizații sau grupări criminale, pentru corupție, fraudă și/sau spălare de bani	Declarație în conformitate cu Anexa nr. 2 autentificată prin aplicarea semnăturii electronice a Participantului – depunere obligatorie după desemnare în calitate de ofertant/ofertant asociat desemnat câștigător;	Da – depunere obligatorie după desemnare în calitate de câștigător

Anexa nr. 2

APROBAT
prin Ordinul
Ministrului Finanțelor
nr. 145 din 24 noiembrie 2020

DECLARAȚIE privind confirmarea identității beneficiarilor efectivi și neîncadrarea acestora în situația condamnării pentru participarea la activități ale unei organizații sau grupări criminale, pentru corupție, fraudă și/sau spălare de bani.

Subsemnatul, _____ reprezentant împuternicit al _____ (*denumirea operatorului economic*) în calitate de ofertant/ofertant asociat desemnat câștigător în cadrul procedurii de achiziție publică nr. _____ din data __/__/__, declar pe propria răspundere, sub sancțiunile aplicabile faptei de fals în acte publice, că beneficiarul/beneficiarii efectivi ai operatorului economic în ultimii 5 ani nu au fost condamnați prin hotărâre judecătorească definitivă pentru participarea la activități ale unei organizații sau grupări criminale, pentru corupție, fraudă și/sau spălare de bani.

Numele și prenumele beneficiarului efectiv	IDNP al beneficiarului efectiv

Data completării: _____
 Semnat: _____
 Nume/prenume: _____
 Funcția: _____
 Denumirea operatorului economic _____
 IDNO al operatorului economic _____

17. **Garanția pentru ofertă, nu se aplică;**
 18. **Garanția de bună execuție a contractului, nu se aplică;**
 19. **Motivul recurgerii la procedura accelerată (în cazul licitației deschise, restrânse și al procedurii negociate), după caz . Nu se aplică**

20. Tehnici și instrumente specifice de atribuire (dacă este cazul specificați dacă se va utiliza acordul-cadru, sistemul dinamic de achiziție sau licitația electronică): **licitația electronică, 3 runde, pasul minim pentru întreaga ofertă 3 800,00 lei.**
21. Condiții speciale de care depinde îndeplinirea contractului (indicați după caz) nu sunt.
22. Ofertele se prezintă în valuta: - **lei moldovenești.**
23. Criteriul de evaluare aplicat pentru adjudecarea contractului: *Cel mai mic preț fără TVA pentru întreaga ofertă.*
24. Factorii de evaluare a ofertei celei mai avantajoase din punct de vedere economic, precum și ponderile lor: Nu se aplică

Nr. d/o	Denumirea factorului de evaluare	Ponderea%
	Nu se aplică	

25. Termenul limită de depunere/deschidere a ofertelor:
Conform informației în SI "RSAP"
26. Adresa la care trebuie transmise ofertele sau cererile de participare:
Ofertele sau cererile de participare vor fi depuse electronic prin intermediul SI RSAP.
27. Termenul de valabilitate a ofertelor: 60 zile
28. Locul deschiderii ofertelor: SI RSAP M-Tender.
Ofertele întârziate vor fi respinse.
29. Persoanele autorizate să asiste la deschiderea ofertelor:
Ofertanții sau reprezentanții acestora au dreptul să participe la deschiderea ofertelor, cu excepția cazului când ofertele au fost depuse prin SI RSAP.
30. Limba sau limbile în care trebuie redactate ofertele sau cererile de participare:
Limba de stat.
31. Respectivul contract se referă la un proiect și/sau program finanțat din fonduri ale Uniunii Europene: Nu se aplică
32. Denumirea și adresa organismului competent de soluționare a contestațiilor:
Agenția Națională pentru Soluționarea Contestațiilor
Adresa: mun. Chișinău, bd. Ștefan cel Mare și Sfânt nr.124 (et.4), MD 2001;
Tel/Fax/email: 022-820 652, 022 820-651, contestatii@ansc.md
33. Data (datele) și referința (referințele) publicărilor anterioare în Jurnalul Oficial al Uniunii Europene privind contractul (contractele) la care se referă anunțul respective (dacă este cazul): Nu se aplică
34. În cazul achizițiilor periodice, calendarul estimat pentru publicarea anunțurilor viitoare: Nu se aplică
35. Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunț: Nu se aplică
36. Data transmiterii spre publicare a anunțului de participare:
Conform informației în SI RSAP.
37. În cadrul procedurii de achiziție publică se va utiliza/accepta:

Denumirea instrumentului electronic	Se va utiliza/accepta sau nu
depunerea electronică a ofertelor sau a cererilor de participare	Se acceptă
sistemul de comenzi electronice	Nu se acceptă
facturarea electronică	Nu se acceptă
plățile electronice	Se acceptă

38. Contractul intră sub incidența Acordului privind achizițiile guvernamentale al Organizației Mondiale a Comerțului (numai în cazul anunțurilor transmise spre publicare în Jurnalul Oficial al Uniunii Europene): Nu se aplică

39. Alte informații relevante:

Președinta grupului de lucru: _____ **Moraru Maia**

L.Ș.

Anexa nr. 7
la Documentația standard nr. _____
din “ _____ ” _____ 20 _____

CERERE DE PARTICIPARE

Către _____
(denumirea autorității contractante și adresa completă)

Stimați domni,

Ca urmare a anunțului/invitației de participare/de preselecție apărut în Buletinul achizițiilor publice și/sau Jurnalul Oficial al Uniunii Europene, nr. din
.. (ziua/luna/anul), privind aplicarea procedurii pentru atribuirea contractului
..... (denumirea contractului de achiziție publică), noi
..... (denumirea/numele ofertantului/candidatului), am luat cunoștință de condițiile și
de cerințele expuse în documentația de atribuire și exprimăm prin prezenta interesul de a
participa, în calitate de ofertant/candidat, neavînd obiecții la documentația de atribuire.

Data completării Cu stimă,

Ofertant/candidat

.....

(semnătura autorizată)

Anexa nr. 8
la Documentația standard nr. _____
din “ _____ ” _____ 20 _____

DECLARAȚIE
privind valabilitatea ofertei

Către _____
(denumirea autorității contractante și adresa completă)

Stimați domni,

Ne angajăm să menținem oferta valabilă, **privind achiziționarea** _____
(se indică obiectul achiziției)
prin procedura de achiziție _____,
(tipul procedurii de achiziție)
pentru o durată de _____ zile, (durata în litere și cifre), respectiv până la data de _____
(ziua/luna/anul), și ea va rămâne obligatorie pentru noi și poate fi acceptată oricând înainte de expirarea perioadei de valabilitate.

Data completării Cu stimă,

Ofertant/candidat

.....

(semnătura autorizată)

Anexa nr. 9
la Documentația standard nr. _____
din “ _____ ” _____ 20 ____

BANCA

(denumirea)

SCRISOARE DE GARANȚIE BANCARĂ
pentru participare cu ofertă la procedura de atribuire a contractului de achiziție publică

Către _____
(denumirea autorității contractante și adresa completă)

cu privire la procedura de atribuire a contractului

(denumirea contractului de achiziție publică)
subsemnații _____,
(denumirea băncii)
Înregistrat la _____,
(adresa băncii)
ne obligăm față de _____ să
(denumirea autorității contractante)
plătim suma de _____, la prima sa cerere scrisă și
(suma în litere și în cifre)

fără ca acesta să aibă obligația de a-și motiva cererea respectivă, cu condiția, ca în cererea sa autoritatea contractantă să specifice că suma cerută de ea și datorată ei este din cauza existenței uneia sau mai multora dintre situațiile următoare:

1. Ofertantul _____
(denumirea ofertantului)
își retrage sau modifică oferta în perioada de valabilitate a acesteia;
Prezenta ofertă rămâne valabilă pentru perioada de timp specificată în Anexa nr.2 Anunțul de Participare, începînd cu data-limită pentru depunerea ofertei, în conformitate cu Anexa nr.2 Anunțul de Participare, și rămâne obligatorie și poate fi acceptată în orice moment până la expirarea acestei perioade;
2. Oferta sa fiind stabilită câștigătoare, ofertantul _____
(denumirea ofertantului)
nu a constituit garanția de bună execuție;
3. Oferta sa fiind stabilită câștigătoare, ofertantul _____
(denumirea ofertantului)
a refuzat să semneze contractul de achiziție publică de bunuri/servicii;

Nu se execută vreo condiție, specificată în documentația de atribuire înainte de semnarea contractului de achiziție publică de bunuri/servicii.

Prezenta garanție este valabilă până la data de _____
Parafată de Banca _____ în ziua ____ luna ____ anul ____
(semnătura autorizată)

Anexa nr. 10
la Documentația standard nr. _____
din “ ____ ” _____ 20 ____

[Banca comercială, la cererea ofertantului câștigător, va completa acest formular pe foaie cu antet, în conformitate cu instrucțiunile de mai jos.]

Data: “ ____ ” _____ 20 ____

Procedura de achiziție Nr.: _____

Oficiul Băncii: _____
[introduceți numele complet al garantului]

Beneficiar: _____
[introduceți numele complet al autorității contractante]

GARANȚIA DE BUNĂ EXECUȚIE

Nr. _____

Noi, [introduceți numele legal și adresa băncii], am fost informați că firmei [introduceți numele deplin al Furnizorului/Prestatorului] (numit în continuare „Furnizor/Prestator”) i-a fost adjudecat Contractul de achiziție publică de livrare/prestare _____ [obiectul achiziției, descrieți bunurile/serviciile] conform anunțului/invitației la procedura de achiziție nr. din _____. 20_ [numărul și data procedurii de achiziție] (numit în continuare „Contract”).

Prin urmare, noi înțelegem că Furnizorul/Prestatorul trebuie să depună o Garanție de bună execuție în conformitate cu prevederile documentației de atribuire.

În urma solicitării Furnizorului/Prestatorului, noi, prin prezenta, ne angajăm irevocabil să vă plătim orice sumă(e) ce nu depășește [introduceți suma(ele) în cifre și cuvinte] la primirea primei cereri în scris din partea Dvs., prin care declarați că Furnizorul/Prestatorul nu îndeplinește una sau mai multe obligații conform Contractului, fără discuții sau clarificări și fără necesitatea de a demonstra sau arăta temeiurile sau motivele pentru cererea Dvs. Sau pentru suma indicată în aceasta.

Această Garanție va expira nu mai târziu de [introduceți numărul] de la data de [introduceți luna][introduceți anul], și orice cerere de plată ce ține de aceasta trebuie recepționată de către noi la oficiu pînă la această dată inclusiv.

[semnăturile reprezentanților autorizați ai băncii și ai Furnizorului/Prestatorului]

Anexa nr. 11
la Documentația standard nr. _____
din “_____” _____ 20____

INFORMAȚII PRIVIND ASOCIEREA

1. Părți contractante (agenți economici)

- a) _____
- b) _____
- c) _____

2. Adrese, telefon, fax a oficiilor partenerilor (părți contractante):

- a) _____
- b) _____
- c) _____

3. Informații privind modul de asociere:

- a) Data încheierii contractului de asociere _____
- b) Locul și data înregistrării asociației _____

c) Activități economice ce se vor realiza în comun

d) Contribuția fiecărei părți la realizarea activităților economice comune convenite

e) Valoarea și cota procentuală a bunurilor livrate/serviciilor prestate de fiecare asociat

f) Condiții de administrare a asociației

g) Modalitatea de împărțire a rezultatelor activității economice comune desfășurate

h) Cauze de încetare a asociației și modul de împărțire a rezultatelor lichidării

i) Repartizarea fizică, valorică și procentuală între fiecare asociat pentru executarea obiectivului supus licitației

j) Alte cauze

Data completării

Semnat Liderul Asociației:

Nume:

Funcția în cadrul firmei:

Denumirea firmei:

Semnat Asociatul secund:

Nume:

Funcția în cadrul firmei:

Denumirea firmei:

Anexa nr. 12
la Documentația standard nr. _____
din “ ” 20__

DECLARAȚIE
privind lista principalelor livrări/prestări efectuate în ultimii 3 ani de activitate

Nr d/o	Obiectul contractului	Denumirea/ numele beneficiarului/Adresa	Calitatea Furnizorului/Prestatorului*)	Prețul contractului/ valoarea bunurilor/serviciilor livrate/prestate	Perioada de livrare/prestare (luni)
1					
2					
...					

*) Se precizează calitatea în care a participat la îndeplinirea contractului, care poate fi de: contractant unic sau lider de asociație; contractant asociat; subcontractant.

Semnat:

Nume:

Funcția în cadrul firmei:

Denumirea firmei:

Anexa nr. 13
la Documentația standard nr. _____
din “ _____ ” _____ 20 ____

DECLARAȚIE
privind dotările specifice, utilajul și echipamentul necesar pentru îndeplinirea
corespunzătoare a contractului

Nr. d/o	Denumirea principalelor utilaje, echipamente, mijloace de transport, baze de producție (ateliere, depozite, spații de cazare) și laboratoare propuse de ofertant ca necesare pentru prestarea serviciilor, rezultate în baza tehnologiilor pe care el urmează să le adopte	Unitatea de măsură (bucăți și seturi)	Asigurate din dotare	Asigurate de la terți sau din alte surse
0	1	2	3	4
1.				
2.				
3.				
.				
n				

Semnat: _____
Nume: _____
Funcția în cadrul firmei: _____
Denumirea firmei: _____

Anexa nr.15
la Documentația standard nr. _____
din “ _____ ” _____ 20 ____

LISTA SUBCONTRACTANȚILOR
ȘI PARTEA/PĂRȚILE DIN CONTRACT CARE SUNT
ÎNDEPLINITE DE ACEȘTIA

Nr. d/o	Numele și adresa subantreprenorilor	Activități din contract	Valoarea aproximativă	% din valoarea contractului
1.				

2.				
3.				
4.				

Semnat: _____

Nume: _____

Funcția în cadrul firmei: _____

Denumirea firmei: _____

Anexa nr.16
la Documentația standard nr. _____
din “ _____ ” _____ 20 _____

ANGAJAMENT TERȚ SUSȚINĂTOR FINANCIAR

Terț susținător financiar

.....(denumirea)

ANGAJAMENT

privind susținerea financiară a ofertantului/candidatului

Către,

(denumirea autorității contractante și adresa completă)

Cu privire la procedura pentru atribuirea contractului

(denumirea contractului de achiziție publică), noi(denumirea terțului susținător financiar), având sediul înregistrat la (adresa terțului susținător financiar), ne obligăm, în mod ferm, necondiționat și irevocabil, să punem la dispoziția (denumirea ofertantului/candidatului) toate resursele financiare necesare pentru îndeplinirea integrală și la termen a tuturor obligațiilor asumate de acesta conform ofertei prezentate și contractului de achiziție publică ce urmează a fi încheiat între ofertant și autoritatea contractantă.

Acordarea susținerii financiare nu implică alte costuri pentru achizitor, cu excepția celor care au fost incluse în propunerea financiară.

În acest sens, ne obligăm în mod ferm, necondiționat și irevocabil, să punem la dispoziția(denumirea ofertantului/candidatului) suma de(valoarea totală/parțială din propunerea financiară), necesară pentru îndeplinirea integrală, reglementară și la termen a contractului de achiziție publică.

Noi, (denumirea terțului susținător financiar), declarăm că înțelegem să răspundem față de autoritatea contractantă pentru neexecutarea oricărei obligații asumate de (denumirea ofertantului), în baza contractului de achiziție publică și pentru care (denumirea ofertantului/candidatului) a primit susținerea financiară

conform prezentului angajament, renunțând în acest sens, definitiv și irevocabil, la invocarea beneficiului de diviziune.

Noi, (*denumirea terțului susținător financiar*), declarăm că înțelegem să renunțăm definitiv și irevocabil la dreptul de a invoca orice excepție de neexecutare, atât față de autoritatea contractantă, cât și față de (*denumirea ofertantului/candidatului*), care ar putea conduce la neexecutarea, parțială sau totală, sau la executarea cu întârziere sau în mod necorespunzător a obligațiilor asumate de noi prin prezentul angajament.

Noi, (*denumirea terțului susținător financiar*), declarăm că înțelegem să răspundem pentru prejudiciile cauzate autorității contractante ca urmare a nerespectării obligațiilor prevăzute în angajament.

Prezentul reprezintă angajamentul nostru ferm încheiat în conformitate cu prevederile art.21 alin.(6) al Legii nr.131/2015 privind achizițiile publice, care dă dreptul autorității contractante de a solicita, în mod legitim, îndeplinirea de către noi a anumitor obligații care decurg din susținerea financiară acordată (*denumirea ofertantului/candidatului*).

Data completării,
.....

Terț susținător,
.....

(*semnătură autorizată*)

Anexa nr. 17

la Documentația standard nr. _____
din “ _____ ” _____ 20 _____

DECLARAȚIE TERȚ SUSȚINĂTOR FINANCIAR

Terț susținător financiar

.....
(denumirea)

Declarație

Subsemnatul, reprezentant împuternicit al (*denumirea terțului susținător financiar*), declar pe propria răspundere, sub sancțiunile aplicabile faptei de fals în acte publice, că toate resursele financiare necesare pentru îndeplinirea integrală și la termen a tuturor obligațiilor contractului de achiziție publică..... sunt reale.

Declar de asemenea că vom disponibiliza aceste resurse necondiționat, în funcție de necesitățile care vor apărea pe parcursul îndeplinirii contractului de achiziție publică având ca obiect.....(*obiectul contractului*).

Data completării,

Terț susținător,

(*semnătură autorizată*)

Anexa nr. 18

la Documentația standard nr. _____
din “ _____ ” _____ 20 _____

**ANGAJAMENT PRIVIND SUSȚINEREA TEHNICĂ ȘI PROFESIONALĂ
A OFERTANTULUI/GRUPULUI DE OPERATORI ECONOMICI**

.....
(denumirea)

**ANGAJAMENT
privind susținerea tehnică și profesională
a ofertantului/candidatului**

Către,

(denumirea autorității contractante și adresa completă)

Cu privire la procedura pentru atribuirea contractului (denumirea contractului de achiziție publică), noi (denumirea terțului susținător tehnic și profesional), având sediul înregistrat la (adresa terțului susținător tehnic și profesional), ne obligăm, în mod ferm, necondiționat și irevocabil, să punem la dispoziția (denumirea ofertantului) toate resursele tehnice și profesionale necesare pentru îndeplinirea integrală și la termen a tuturor obligațiilor asumate de acesta, conform ofertei prezentate și contractului de achiziție publică ce urmează a fi încheiat între ofertant și autoritatea contractantă.

Acordarea susținerii tehnice și profesionale nu implică alte costuri pentru achizitor, cu excepția celor care au fost incluse în propunerea financiară.

În acest sens, ne obligăm în mod ferm, necondiționat și irevocabil, să punem la dispoziția (denumirea ofertantului/candidatului) resursele tehnice și/sau profesionale de necesare pentru îndeplinirea integrală, reglementară și la termen a contractului de achiziție publică.

Noi, (denumirea terțului susținător tehnic și profesional), declarăm că înțelegem să răspundem, în mod necondiționat, față de autoritatea contractantă pentru neexecutarea oricărei obligații asumate de (denumirea ofertantului/candidatului), în baza contractului de achiziție publică, și pentru care (denumirea operatorului/candidatului) a primit susținerea tehnică și profesională conform prezentului angajament, renunțând în acest sens, definitiv și irevocabil, la invocarea beneficiului de diviziune.

Noi, (denumirea terțului susținător tehnic și profesional), declarăm că înțelegem să renunțăm definitiv și irevocabil la dreptul de a invoca orice excepție de neexecutare, atât față de autoritatea contractantă, cât și față de (denumirea ofertant), care ar putea conduce la neexecutarea, parțială sau totală, sau la executarea cu întârziere sau în mod necorespunzător a obligațiilor asumate de noi prin prezentul angajament.

Noi, (denumirea terțului susținător tehnic și profesional), declarăm că înțelegem să răspundem pentru prejudiciile cauzate autorității contractante ca urmare a nerespectării obligațiilor prevăzute în angajament.

Prezentul reprezintă angajamentul nostru ferm încheiat în conformitate cu prevederile art.22 alin.(6) al Legii nr.131/2015 privind achizițiile publice, care dă dreptul autorității contractante de a solicita, în mod legitim, îndeplinirea de către noi a anumitor obligații care decurg din susținerea tehnică și profesională acordată (denumirea ofertantului/candidatului).

Data completării,

.....

Terț susținător,

.....

(semnătură autorizată)

DECLARAȚIE TERȚ SUSȚINĂTOR TEHNIC

Terț susținător tehnic

.....
(denumirea)

Declarație

Subsemnatul, reprezentant împuternicit al (*denumirea terțului susținător tehnic*), declar pe propria răspundere, sub sancțiunile aplicabile faptei de fals în acte publice, că datele prezentate în tabelul anexat privind logistica, utilajele, instalațiile, echipamentele tehnice de care dispun și care urmează a fi folosite efectiv pentru îndeplinirea contractului de achiziție publică..... sunt reale.

Declar de asemenea că vom disponibiliza aceste resurse necondiționat, în funcție de necesitățile care vor apărea pe parcursul îndeplinirii contractului de achiziție publică având ca obiect.....(*obiectul contractului*).

LISTA

privind logistica, utilajele, instalațiile și echipamentele tehnice aflate în dotare și care urmează a fi efectiv folosite pentru îndeplinirea contractului de achiziție publică

Nr. crt	Denumire utilaj/echipament/instalație	Cantitate U.M.	Forma de deținere	
			Proprietate	În chirie

Prezenta declarație este anexă la „Angajamentul ferm” privind susținerea noastră tehnică și profesională oferită.....(*denumirea ofertantului/candidatului*).

Data completării,

Terț susținător,

(*semnătură autorizată*)

DECLARAȚIE TERȚ SUSȚINĂTOR PROFESIONAL

Terț susținător profesional

.....
(denumirea)

Declarație

Subsemnatul, reprezentant împuternicit al(denumirea terțului susținător profesional), declar pe propria răspundere, sub sancțiunile aplicabile faptei de fals în acte publice, că datele prezentate în tabelul anexat privind efectivul mediu anual al personalului de specialitate angajat care urmează a fi efectiv alocat pentru îndeplinirea contractului de achiziție publică..... sunt reale.

LISTA

privind personalul de specialitate angajat care urmează a fi efectiv
alocat pentru îndeplinirea contractului de achiziție publică

	Anul 1	Anul 2	Anul 3
Personalul de specialitate			
.....			
.....			
.....			

Anexez declarației, CV-urile personalului de specialitate, precum și ale personalului care va fi alocat efectiv pentru îndeplinirea contractului de achiziție publică.

Subsemnatul declar că informațiile furnizate, referitoare la experiența anterioară, capacitățile tehnice și personalul de specialitate angajat sunt complete și corecte în fiecare detaliu și înțeleg că autoritatea contractantă are dreptul de a solicita, în scopul verificării și confirmării declarațiilor, situațiilor și documentelor care însoțesc oferta, orice informații suplimentare în scopul verificării datelor din prezenta declarație.

Subsemnatul autorizez prin prezenta orice instituție, societate comercială, bancă, alte persoane juridice să furnizeze informații reprezentanților autorizați ai
(denumirea și adresa autorității contractante) cu privire la orice aspect tehnic și financiar în legătură cu activitatea noastră.

Prezenta declarație este anexă la „Angajamentul ferm” privind susținerea noastră tehnică și profesională oferită
.....(denumirea ofertantului/candidatului).

Data completării,

Terț susținător,

(semnătură autorizată)

Anexa nr. 21
la Documentația standard nr. _____
din “_____” _____ 20____

CAIET DE SARCINI Bunuri/Servicii

Obiectul _____
(denumirea, adresa)

Autoritatea contractantă _____
(denumirea, adresa)

1. Descriere generală. Informații

Se dau detalii generale privind obiectul achiziției.

2. Utilizarea, păstrarea, protecția, calitatea produselor/serviciilor

Se precizează detalii privind modul de transportare, prestare, utilizare și locul livrării/prestării a produselor/serviciilor.

3. Materiale, compatibilități, reglementări tehnice și standarde utilizate

Se precizează conformitatea și aplicabilitatea materialelor, legislația, reglementările tehnice și standardele aplicate.

4. Cerințe privind calculul costului/prețului

Se precizează modalitatea de calculare a costului bunului/serviciului, prin trimitere la actele normative în domeniu.

5. Mostre

Se precizează modul de prezentare a mostrelor la toate produsele utilizate.

6. Echipamentele, instalațiile, utilajele, sculele, instrumentele, dispozitivele și alte obiecte necesare pentru prestarea serviciilor

Se precizează echipamentele, instalațiile, utilajele, sculele, instrumentele, dispozitivele, mijloacele de transport, etc..

7. Articole, produse și piese necesare instalațiilor

Se precizează furnizorul articolelor, produselor și pieselor necesare instalațiilor, tipurile și cantitatea.

8. Definiții

Se precizează termenii și definițiile utilizate în caietul de sarcini și unele caracteristici.

9. Documente obligatorii la depunerea ofertei

La punctul dat autoritatea contractantă indică care documente sunt obligatorii de a fi prezentate la depunerea ofertei prin intermediul SIA RSAP. La fel, tot aici se indică documentele ce conțin date cu caracter personal, care nu se depun prin intermediul SIA RSAP și nu sunt publice pentru toți.

10. Documente obligatorii la evaluarea ofertelor

La punctul dat autoritatea contractantă indică care documente sunt obligatorii de a fi prezentate în SIA RSAP la evaluarea ofertei. La fel, tot aici se indică documentele ce conțin date cu caracter personal, care nu se depun prin intermediul SIA RSAP și nu sunt publice pentru toți, ele se prezintă la etapa de evaluare direct autorității contractante.

Autoritatea contractantă _____ Data „____” _____

Notă: Prezentul model al caietului de sarcini este orientativ și poate fi completat, modificat, precizat de către autoritatea contractantă, în funcție de tipul și specificul bunurilor/serviciilor. Autoritatea contractantă este obligată să respecte legislația.

Specificații tehnice

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7, iar de către autoritatea contractantă – în coloanele 1, 5,]

Numărul procedurii de achiziție _____	din _____
Obiectul achiziției: _____	

Denumirea serviciilor	Denumirea modelului serviciului	Țara de origine	Produsul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
<u>Echipamente de rețea de tip Next Generation Firewall (NGFW)</u>						
<u>Echipamente de rețea de tip Next Generation Firewall (NGFW)</u>				Echipamente de rețea de tip Next Generation Firewall (NGFW) Cerințe tehnice 1. Protecția rețelei cu controlul stării sesiunilor; 2. Recunoașterea și blocarea aplicațiilor de rețea la nivelul 7 al modelului OSI în funcție de traficul care trece prin firewall, inclusiv individual pentru toate aplicațiile care folosesc porturi comune, inclusiv 80 și 443, precum și pentru aplicațiile care utilizează porturi TCP/UDP dinamice; 3. Firewall-ul NGFW propus trebuie să fie certificat minim conform standardelor ISO 27001, ISO 27017, ISO 27018, ISO 27701, Germany C5, Common Criteria, FIPS 140-2, CMVP. 4. Firewall-ul NGFW propus nu trebuie să necesite o repornire pentru a verifica și instala actualizările de securitate. 5. Firewall-ul NGFW propus trebuie să poată identifica aplicațiile indiferent de portul utilizat, criptarea SSL/SSH sau metodele de ocolire folosite. 6. Firewall-ul NGFW propus trebuie să clasifice aplicațiile neidentificate pentru gestionarea politicii, analiza criminalistică a amenințărilor sau dezvoltarea tehnologiilor de identificare a aplicațiilor. 7. Firewall-ul NGFW propus trebuie să fie o soluție dezvoltată inițial pentru asigurarea securității (nu un management de aplicații cu un firewall de bază care verifică starea). 8. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas. 9. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas. 10. Firewall-ul NGFW propus trebuie să poată să delimiteze diferite părți ale unei		Moldova Standard

				aplicații, cum ar fi permiterea chat-ului pe Facebook, dar blocarea posibilității de a trimite fișiere. 11. Firewall-ul NGFW propus trebuie să controleze accesul și să aplice politici pentru site-uri web și aplicații, inclusiv pentru aplicațiile SaaS. 12. Firewall-ul NGFW propus trebuie să utilizeze un sistem de operare unificat în toate formatele. 13. Firewall-ul NGFW propus trebuie să sprijine crearea politicii de securitate pentru prevenirea furtului de credențiale. 14. Firewall-ul NGFW propus trebuie să sprijine aplicarea autentificării multi-factor pentru aplicațiile interne. 15. Firewall-ul NGFW propus trebuie să permită vizibilitatea și controlul aplicațiilor care folosesc porturi non-standard, într-o politică unică de securitate. 16. Firewall-ul NGFW propus trebuie să poată oferi algoritmi de învățare automată pentru protecție avansată direct din NGFW, fără a necesita conexiuni externe. 17. Recunoașterea în traficul inspectat la Layer-7 al modelului OSI a semnăturilor stocate pe MFE pentru următoarele categorii de aplicații: 17.1 . Aplicații corporative: 17.1.1. Servicii de autentificare, inclusiv Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS; 17.1.2. Sisteme de gestionare a bazelor de date (SGBD), inclusiv Microsoft SQL, Oracle, DB2, Postgres, Sybase; 17.1.3. Servicii de fișiere, inclusiv Microsoft SMB. 17.1.4. ERP, CRM, inclusiv SAP, 1C; 17.1.5. Sisteme de management al documentelor electronice și schimb de mesaje, inclusiv EMC Documentum, Microsoft SharePoint, Exchange, Lync, Office 365, Google Docs, Lotus; 17.1.6. Protocoale de schimb de e-mail: SMTP, POP3, IMAP; 17.1.7. Protocoale VoIP și conferințe audio-video, inclusiv SIP, H.323, H.245, H.225, Webex; 17.1.8. Servicii de actualizare software, inclusiv Microsoft Update, software antivirus (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple; 17.1.9. Servicii de backup, inclusiv Symantec Backup Exec; 17.1.10. Servicii de virtualizare și acces la terminale, inclusiv VMware, Citrix, Microsoft RDP; 17.1.11. Alte protocoale și tehnologii utilizate pentru crearea aplicațiilor distribuite, inclusiv CORBA, SOAP; 17.1.12. Protocoale de acces de la distanță, inclusiv Telnet, SSH, VNC, Radmin; 17.1.13. Protocoale de rețea, inclusiv protocoale de rutare dinamică și SSL, IPsec VPN; 17.2. Aplicații Internet: 17.2.1. E-mail, inclusiv Gmail,		
--	--	--	--	--	--	--

				Yandex.Mail, Mail.ru, Hotmail; 17.2.2. Rețele sociale, inclusiv Facebook, Google+, LinkedIn, ВКонтакте, Odnoklassniki, „Moy Mir”; 17.2.3. Servicii de mesagerie instantanee, inclusiv Jabber, IRC, MSN, servicii similare în cadrul rețelelor sociale enumerate mai sus; 17.2.4. Servicii de conferință audio-video 17.2.5. Servicii de schimb de fișiere prin HTTP(S) și peer-to-peer, inclusiv Dropbox, BitTorrent, eMule, Google Drive, Yandex Disk, Gnutella, Boxnet, WebDav; 17.2.6. Streaming audio-video (indiferent de site-ul web), inclusiv YouTube, Vimeo, audio și video prin HTTP; 17.2.7. Servicii de publicare a desktop-ului și oferirea de acces de la distanță, inclusiv TeamViewer, LogMeIn; 17.2.8. Proxy externe și anonimizatoare, inclusiv Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy; 17.2.9. Servicii de construire a VPN-urilor private și tuneluri deasupra altor aplicații, inclusiv FreeNet, Open-VPN, VTun, RDP-to-TCP, TCP-over-DNS; 18. Oferirea de instrumente integrate în MFE pentru crearea semnăturilor proprii de aplicații bazate pe expresii regulate folosind decodare pentru HTTP(S), FTP, SMB, SMTP, RPC și altele, precum și pe mască pentru conținutul pachetelor TCP/UDP; 19. Recunoașterea aplicațiilor transmise prin protocolul HTTP/2; 20. Recunoașterea aplicațiilor de rețea prin traficul criptat SSL (suport pentru chei RSA de până la 2048 de biți) și SSHv2 care trece prin firewall (decriptarea SSL, SSHv2) – atât pentru conexiunile intrante, cât și pentru cele ieșite, transparent pentru utilizatori în domeniu, cu posibilitatea de a controla funcțiile individuale ale aplicațiilor, inclusiv trimiterea de mesaje pe rețelele sociale, schimbul de fișiere, streaming audio și video; 21. Inspecția tunelurilor: 21.1. Generic Routing Encapsulation (GRE) (RFC 2784); 21.2. Trafic IPSec necriptat [NULL Encryption Algorithm pentru IPSec (RFC 2410)]; 21.3. Mod de transport AH IPSec. 22. Recunoașterea secvențială a diferitelor aplicații utilizate într-o singură sesiune; 23. Recunoașterea utilizatorilor care folosesc aplicații de rețea prin integrarea cu serviciile corporative de autentificare a utilizatorilor, cum ar fi Microsoft Active Directory, Microsoft Exchange, Novell eDirectory, LDAP, Citrix; posibilitatea integrării cu alte servicii de autentificare (de exemplu, controlerele de rețea wireless) printr-o API XML deschisă; posibilitatea de a utiliza autentificarea forțată a utilizatorilor folosind o pagină WEB – „Captive portal”; suport pentru Kerberos, Tacacs+, SAML v.2, suport pentru roaming-ul L3 al		
--	--	--	--	---	--	--

				utilizatorilor prin sondaje WMI și NetBios; 24. Inspecția în timp real a conținutului traficului transmis prin firewall pe baza semnăturilor și comportamentului, protecția împotriva vulnerabilităților, atacurilor de rețea și a malware-ului, recunoașterea tipurilor de fișiere pe baza semnăturilor acestora, detectarea virusilor transmiși prin web, e-mail, FTP, SMB, spyware, viermi de rețea, blocarea transmișiei unor conținuturi specifice folosind expresii regulate, inclusiv pentru aplicațiile care utilizează criptare SSL și SSHv2; 25. Crearea de reguli pentru traficul care trece prin firewall într-o politică unificată de securitate, utilizând următorii parametri pentru fiecare conexiune: 25.1. Adresa IP a expeditorului, 25.2. Adresa IP a destinatarului, 25.3. Serviciile L4 utilizate: porturi pentru protocoalele TCP și UDP, 25.4. Numele utilizatorilor sau grupurilor de utilizatori din Active Directory, 25.5. Aplicațiile la nivelul 7 al modelului OSI, 25.6. URL categorii. 26. Crearea de reguli într-o politică unificată de securitate, utilizând ca parametri informațiile despre adresele IP ale expeditorului, destinatarului, serviciile utilizate (porturi TCP/UDP), numele utilizatorilor, grupurilor de utilizatori și aplicațiile utilizate de aceștia sau anumite categorii de aplicații. În politicile create, trebuie să existe posibilitatea implementării următoarelor acțiuni: • Permisie sau interdicție; • Permisie sau interdicție pentru un anumit aplicații sau categorii de aplicații de a utiliza doar porturi TCP/UDP standard sau strict definite. Aceste porturi nu trebuie să fie folosite de alte aplicații fără o politică care să permită explicit astfel de interacțiuni; • Permisie sau interdicție pentru scanare pentru virusi și alte amenințări; • Permisie sau interdicție pe bază de orar, utilizator sau grup de utilizatori; • Decriptare și verificare. Dacă nu s-a putut decripta (în cazul unui algoritm criptografic nestandard, certificat expirat etc.) – interzicere; • Ne-decriptarea anumitor categorii de URL și site-uri web de încredere; • Aplicarea marcatului DSCP și limitarea traficului folosind politici QoS bazate pe aplicații, adrese IP, utilizatori și grupuri de utilizatori; • Implementarea hardware a QoS pentru traficul real-time, identificat la nivelul aplicațiilor; • Aplicarea redirecționării traficului pe bază de politici (Policy Based Forwarding); • Permisie sau interdicție pentru anumite funcții ale aplicației; • Oricare combinație dintre acțiunile de mai sus.		
--	--	--	--	---	--	--

				27. Protecție antivirus, protecție împotriva software-ului spyware, protecție împotriva vulnerabilităților și atacurilor de rețea (sistem de detecție și prevenire a intruziunilor), filtrare URL utilizând o bază dinamică de reputație, care susține categorizarea diferitelor secțiuni ale aceluiși site web, inclusiv susținerea categoriilor pentru site-uri web în limba rusă, blocarea transferului de fișiere pe baza tipurilor definite de semnături; 28. Posibilitatea de a verifica suplimentar traficul pentru amenințări necunoscute prin analiza acestuia utilizând tehnologia învățării automate prin servicii cloud; 29. Detectarea și filtrarea solicitărilor către resursele din rețea în funcție de categoria acestora, de exemplu, site-uri malware, rețele sociale, resurse publicitare etc.; 30. Suport pentru acțiuni: permisiune, notificare, blocare, solicitarea confirmării utilizatorului, solicitarea parolei utilizatorului; 31. Filtrarea URL trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 32. Analiza SNI în TLS Hello simultan cu URL-ul în cererea HTTP pentru a contracara tehnicile de ocolire de tip SNIcat; 33. Analiza cererilor DNS suspecte, domeniilor DGA și localizarea stațiilor infectate utilizând tehnologia DNS sinkhole (modificarea răspunsului serverului DNS); 34. Detectarea tehnicilor de ocolire a protecției prin cereri DNS care încearcă să folosească domenii generate automat (DGA), inclusiv analiza frecvenței n-gramelor, analiza entropiei, frecvența cererilor, tunelarea în DNS, canale de transfer de date prin cereri DNS, inclusiv tuneluri DNS ultra-lente; 35. Blocarea domeniilor DGA, domeniilor DGA create pe baza unui dicționar, tehnici de ocolire DNS-rebinding, FastFlux, interogări către înregistrări DNS suspendate, atacuri NSNX, atacuri cu domenii recent înregistrate; 36. Analiza cererilor DNS suspecte trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 37. Protecție împotriva tehnicilor de evitare (evasions), de exemplu MPTCP; 38. Oferirea unui serviciu de scanare a fișierelor potențial dăunătoare necunoscute în sandbox cu sisteme de operare Microsoft Windows, Linux prin metoda de emulare a rulării și vizualizare a documentelor; 39. Sandbox-ul trebuie să verifice fișierele executabile suspecte (inclusiv EXE, DLL, SCR, BAT, etc.), fișiere ELF, documente în formatele PDF, MS Office 2007, 2010, 2016 și mai sus, Java și Flash, Android APK, Mach-O, DMG și PKG, arhive RAR, ZIP, 7Zip;	
--	--	--	--	--	--

				40. Firewall-ul trebuie să trimită spre verificare în sandbox fișierele suspecte transmise prin aplicațiile HTTP, SMTP, POP3, IMAP, SMB, FTP, precum și implementările acestora prin SSL, dacă există; 41. Sandbox-ul trebuie să genereze și să trimită către firewall un raport despre verificarea fișierului; 42. Sandbox-ul trebuie să genereze semnături pentru blocarea atacurilor de tip zero-day pentru utilizarea pe toate firewall-urile companiei în aplicațiile enumerate, în decurs de 5 minute de la primirea fișierului pentru verificare; 43. Firewall-ul trebuie să primească semnăturile fișierelor din sandbox și să aibă un motor de blocare bazat pe noile semnături obținute de la sandbox-ul cloud sau local; 44. Sandbox-ul furnizorului cloud trebuie să aibă posibilitatea de a schimba semnături între toți clienții furnizorului; 45. Firewall-ul trebuie să primească din sandbox indicatori de compromitere: IP, URL, DNS, care sunt utilizate de codul malițios și să blocheze conexiunile pe baza listei de indicatori malițioși. 46. Sandbox-ul trebuie să verifice linkurile HTTP:// și HTTPS:// din e-mailuri prin protocoalele SMTP/POP3. 47. Sandbox-ul trebuie să verifice fișierele din aplicațiile criptate SSL, cel puțin în protocolul HTTPS. 48. Suport obligatoriu pentru învățarea automată în timpul inspecției amenințărilor de tip zero-day pentru a reduce întârzierea în inspecția fișierelor suspecte; 49. Sandbox-ul trebuie să asigure analiza comportamentului fișierelor și linkurilor suspecte în cloud privat sau extern (sandbox), să detecteze noi malware și să genereze automat semnături antivirus în decurs de 5 minute și să actualizeze baza de reputație URL în decurs de 30 de minute, care se vor instala pe toate dispozitivele Clientului cu abonamentele corespunzătoare; 50. Posibilitatea integrării cu subsistemul de detectare a amenințărilor zero-day, implementat pe un dispozitiv hardware dedicat aceluiași furnizor, plasat pe obiectul central al Clientului (cloud privat), care permite generarea automată a semnăturii antivirus local, pe dispozitivul hardware dedicat în centrul de date (DC) al Clientului în decurs de 5 minute; 51. Sandbox-ul local dedicat trebuie să aibă un API pentru primirea fișierelor spre verificare atât de la firewall-uri, cât și de la servicii terțe; 52. Sandbox-ul trebuie să genereze rapoarte despre verificările efectuate și să permită vizualizarea acestora în format PDF; 53. Sandbox-ul cloud trebuie să utilizeze tehnologia Bare Metal Analysis fără a utiliza emularea sistemului de		
--	--	--	--	--	--	--

				operare; 54. Firewall-ul trebuie să aibă capacitatea de a trimite fișiere diferite în sandbox-uri diferite, de exemplu, fișierele EXE în sandbox-ul cloud, iar fișierele DOC în sandbox-ul local; 55. Sandbox-ul cloud trebuie să accepte fișiere PE pentru verificare, chiar și în absența unui abonament; 56. Suport pentru următorii furnizori de autentificare multi-factor (Multi-Factor Authentication - MFA) (direct, fără utilizarea produselor intermediare): Duo, • Oka, • RSA SecureID, • PingID; 57. Protecție împotriva furtului de loginuri și parole ale utilizatorilor prin integrarea cu Active Directory (AD), monitorizarea transmiției conturilor de utilizator către zone de securitate neîncredere, autentificarea forțată a utilizatorilor prin autentificare cu doi factori (MFA); 58. Funcționalitate de control granular al accesului utilizatorilor de la distanță în mediul de lucru corporativ, cu posibilitatea de verificare a existenței anumitor software-uri pe stația de lucru a utilizatorului și accesul prin dispozitive mobile; 59. Funcționalitate de protecție împotriva atacurilor DoS; 60. Posibilitatea de a activa 100% din semnăturile IPS, antivirus, filtrarea URL-urilor, controlul aplicațiilor și Threat Intelligence fără a degrada performanța; 61. Funcționalitate de blocare a scanării porturilor ICMP/TCP/UDP; 62. Detectarea obiectelor din fișierele transmise prin rețea care conțin informații importante și blocarea transmiției acestor fișiere; 63. Detectarea prezenței datelor filtrabile în fișierele transmise prin rețea, incluzând, dar fără a se limita la: Adobe PDF, HTML, Microsoft Office (Excel, Word, PowerPoint). Rich Text Format; 64. Prezența șabloanelor de date preconfigurate, cum ar fi numerele de carduri de credit. 65. Suport pentru crearea de șabloane proprii de date pe baza expresiilor regulate. 66. Posibilitatea de integrare cu subsistemul de management centralizat, logare, raportare și actualizare a software-ului pentru firewall-uri de același furnizor. 67. Cerințe pentru sistemul de management centralizat: • Funcționalități avansate de vizualizare a activității aplicațiilor rețelei, amenințărilor rețelei detectate și blocate, utilizarea aplicațiilor de către utilizatori. Permite filtrarea informațiilor pe aplicații, amenințări, utilizatori, adrese IP, porturi TCP/UDP, zone de securitate, tipuri de amenințări etc.; • Corelarea automată a jurnalelor	
--	--	--	--	---	--

				de diferite tipuri, generate în cadrul aceleiași sesiuni (filtrarea traficului prin firewall, protecția împotriva amenințărilor, controlul transferului de fișiere, filtrarea URL); • Posibilitatea de corelare automată a evenimentelor de securitate folosind obiecte de corelare actualizabile care folosesc informații de la protecția antivirus, protecția împotriva software-ului spyware, protecția împotriva vulnerabilităților și atacurilor, amenințările de tip zero-day; • Funcționalități de generare automată a rapoartelor și de generare a rapoartelor pe bază de program, cu opțiuni de personalizare manuală a rapoartelor. Rapoartele trebuie să fie vizibile prin interfața grafică (GUI) și să poată fi exportate în formate PDF și CSV. • Posibilitatea de a configura funcționalitățile SD-WAN prin consola de management centralizat. • Sistemul trebuie să poată exporta logurile către soluții externe prin syslog, utilizând formate standardizate precum CEF sau LEEF; • Trebuie să existe mecanisme de inițializare automată pentru echipamente noi, inclusiv în locații la distanță, fără intervenție manuală; • Trebuie să fie posibilă actualizarea centralizată a software-ului pentru echipamentele administrate, într-un mod simplificat; • Soluția trebuie să ofere interfețe moderne de integrare (REST API) compatibile cu XML și JSON, pentru interoperabilitate cu alte sisteme. • Fiecare administrator trebuie să poată face modificări izolate, cu salvare separată, pentru a evita suprascrierea neintenționată; • Sistemul trebuie să permită definirea de roluri și permisiuni personalizate pentru utilizatori, cu acces diferențiat la funcționalități. • Platforma trebuie să permită organizarea echipamentelor și configurațiilor prin grupuri, ierarhii și etichete; • Sistemul trebuie să suporte funcționare în mod redundant (high availability) și echilibrare a sarcinii (load balancing); 68. Posibilitatea de a detecta și analiza traficul dispozitivelor IoT folosind algoritmi de învățare automată. 69. Funcționalitatea de a trimite traficul SSL decriptat către dispozitive externe. 70. Funcționalitatea de a captura traficul de la dispozitive externe și de a-l cripta într-un tunel SSL pentru transmiterea prin Internet. 71. Prezența unui raport separat pentru aplicațiile de tip SaaS. 72. Funcționalitatea IPSec VPN. 73. Integrarea cu sistemele externe SIEM/SIM prin protocolul Syslog, cu configurare flexibilă a formatului	
--	--	--	--	--	--

				jurnalelor. 74. Suport pentru rutare statică și protocoale de rutare dinamică BGP, OSPF, RIP. 75. Suport pentru diverse moduri de lucru ale interfețelor rețelei (monitorizare trafic mirroring, mod transparent, Layer 2 și Layer 3). 76. Suport pentru IPv6, inclusiv identificarea aplicațiilor și utilizatorilor. 77. Suport pentru multicast, incluzând PIM-SM, PIM-SSM, IGMP v1, v2, v3. 78. Suport pentru rutarea între VLAN-uri. 79. Suport pentru NAT, DHCP și DHCP relay. 80. Suport pentru etichetarea cadrelor prin 802.1Q (minim 4094 VLAN-uri). 81. Suport pentru agregarea interfețelor prin 802.3ad (suport LACP). 82. Suport pentru pachete mari (Jumbo frames). 83. Managementul rolurilor administratorilor locali: • Posibilitatea de a restricționa vizualizarea și gestionarea la nivelul dispozitivului și al sistemelor virtuale (contexte); • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la orice secțiune a interfeței web; • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la CLI-ul firewall-ului. 84. Firewall-ul hardware trebuie să dispună de o platformă hardware specializată, care să permită administrarea dispozitivului fără întreruperi, chiar și în condiții de încărcare maximă. Trebuie să fie asigurate resurse de procesare dedicate, separate pentru analiza traficului monitorizat și pentru activitățile de management. Administrarea fiecărui dispozitiv în parte trebuie să se realizeze prin protocoalele HTTPS și SSH, fără a necesita instalarea vreunui software suplimentar de administrare pe stația de lucru a administratorului. Interfața de administrare a firewall-urilor (web și CLI) trebuie să fie unificată cu subsistemul de management centralizat, jurnalizare, raportare și actualizare a software-ului. Cerințe de performanță ale firewall-ului: Performance: • Threat prevention throughput 1.2 Gbps; • IPsec VPN throughput 800 Mbps; • Connections per second 1100; • Firewall throughput 1.4 Gbps; Policies: • Security rules min 500; • Security rule schedules min 256;		
--	--	--	--	--	--	--

				• NAT rules min 400; • Tunnel content inspection rules 100; • SD-WAN rules min 100; • Policy based forwarding rules min 100; • DoS protection rules min 100. Security Zones: • security zones 25. Security Profiles: • Security profiles min 75. URL Filtering: • Total entries for allow list, block list and custom categories 25,000; Interfaces: • I/O: 1G RJ45 (7); • Management I/O: 10/100/1000 out-of-band management port (1), RJ45 console port (1), USB port (1). Storage Capacity: • 128 GB Virtual Routers: • Virtual routers 3. Routing: • IPv4 forwarding table size min 5,000; • IPv6 forwarding table size min 2500; • System total forwarding table size min 5,000; L2 Forwarding: • ARP table size per device 1500; • IPv6 neighbor table size 1500; • MAC table size per device 1500; Address Assignment: • DHCP servers 3; • DHCP relays 500; • IPSec VPN: • Suport Site to site over gre IPSec tunnels • SD-WAN IPsec tunnels 85. Alte cerințe obligatorii: - Garanție, Mentenanță și Suport HW+SW incluse – 12 luni; - Producătorul trebuie să ofere suport prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului; - Ofertantul va indica în ofertă costul serviciilor pentru efectuarea instalării și configurării a echipamentului ofertat, va asigura integrarea echipamentului ofertat cu dispozitivele existente pe baza platformei existente în cadrul instituției prin realizarea configurărilor necesare, cu setarea tuturor parametrilor aplicabili în corespundere cu cerințele înaintate pe infrastructura Beneficiarului. - Prezentarea a certificatelor a minim 1 specialist pe produsul ofertat din partea ofertantului (fără asociere cu o alta companie); - Ofertantul va prezenta copia Certificatului ISO 27001:2018, în domeniul		
--	--	--	--	---	--	--

				serviciilor privind asigurarea securității informației, design-ul acestuia, implementarea, monitorizarea și managementul infrastructurii IT - Ofertantul va prezenta Certificatului ISO 9001:2015, pentru Servicii de comercializare și implementare suport tehnic în garanție și post garanție pentru sisteme informaționale, echipamente hardware și software și Servicii privind asigurarea securității informației, designul, implementarea, monitorizarea și managementul infrastructurii IT și de Securitate – certificat confirmat cu aplicarea semnăturii electronice; - Ofertantul va prezenta Autorizarea de la producător pentru licitația la care participa; - Ofertantul va avea minim o persoană certificată în calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013; - Referințe de vânzare NGFW – minim 3 contracte; - Termen de livrare: maxim până la 90 zile de la data intrării în vigoare a contractului		
TOTAL						

Semnat: _____ Numele, Prenumele: _____ În calitate de:

Ofertantul: _____ Adresa: _____

Anexa nr.23
la Documentația standard nr. _____
din “ ” 20

Specificații de preț										
<i>[Acest tabel va fi completat de către ofertant în coloanele 5,6,7,8 și 11 la necesitate, iar de către autoritatea contractantă – în coloanele 1,2,3,4,9,10]</i>										
Numărul procedurii de achiziție _____ din _____										
Obiectul de achiziție: _____										
Cod CPV	Denumirea bunurilor/serviciilor	Unitatea de măsură	Cantitatea	Preț unitar (fără TVA)	Preț unitar (cu TVA)	Sumă fără TVA	Sumă cu TVA	Termenul de livrare/prestare	Clasificație bugetară (IBAN)	Discount %
1	2	3	4	5	6	7	8	9	10	11
<u>Echipamente de rețea de tip Next Generation Firewall (NGFW)</u>										
32420000-3	<u>Echipamente de rețea de tip Next Generation Firewall (NGFW)</u>	buc	10					<u>Timp de 90 zile din data înaintării comunicării către Vânzător privind transmiterea dării de seamă la Agenția Achiziții Publice, cu livrare și descărcare a bunurilor la depozitul CNAS din str. Gheorghe</u>	MD84TRPFAH518 710A01691AA	

								<u>Tudor nr. 3 mun. Chişinău, cu recepţionarea de către persoana responsabilă desemnată din cadrul CNAS</u>		
--	--	--	--	--	--	--	--	---	--	--

Semnat: _____ Numele, Prenumele: _____ În calitate de:

Ofertantul: _____ Adresa: _____

Anexa nr. 24
la Documentaţia standard nr. _____
din “ ” 20__



CONTRACT Nr.
privind achiziția de bunuri

I PARTEA GENERALĂ

Obiectul achiziției : Echipamente de rețea de tip Next Generation Firewall (NGFW)

Cod CPV: 32420000-3

“ ” 2026

mun. Chişinău

Vânzător	Cumpărător
_____, (denumirea completă a întreprinderii, asociației, organizației) reprezentată prin _____, (funcția, numele, prenumele) care acționează în baza _____, (statut, regulament, hotărâre etc.) denumit(a) în continuare Vânzător, _____, (se indică nr. și data de înregistrare în Registrul de Stat)	<u>Casa Națională de Asigurări Sociale,</u> reprezentată prin <u>Directoare generală</u> <u>Dna ȚÎBÎRNĂ Elena,</u> care acționează în baza regulamentului cu privire la organizarea și funcționarea Casei Naționale de Asigurări Sociale (HG. 230/2020), înregistrat la camera înregistrării de stat IDNO 1004600030235

pe de o parte,	denumit(a) în continuare <i>Cumpărător</i> , pe de altă parte,
----------------	---

ambii (denumiți(te) în continuare Părți), au încheiat prezentul Contract referitor la următoarele:

a) Achiziționarea Echipamente de rețea de tip Next Generation Firewall (NGFW)

(denumirea bunului/serviciului)

denumite în continuare Bunuri, conform procedurii de achiziții publice de tip _____
nr. _____ din _____, în baza deciziei grupului de lucru al Cumpărătorului din
„___” _____ 20__.

b) Următoarele documente vor fi considerate părți componente ale Contractului:

Specificația tehnică..... **Anexa nr.1;**

Specificația de preț..... **Anexa nr.2;**

Act de primire /predare **Anexa nr.3.**

c) În cazul unor discrepanțe sau inconsecvențe între documentele componente ale Contractului, documentele vor avea ordinea de prioritate enumerată mai sus.

d) În calitate de contravaloare a plăților care urmează a fi efectuate de către Cumpărător, Vanzătorul se obligă, prin prezentul contract, să livreze Cumpărătorului Bunurile și să înlăture defectele lor în conformitate cu prevederile Contractului sub toate aspectele.

e) Cumpărătorul se obligă, prin prezentul contract, să plătească Vanzătorului, în calitate de contravaloare a livrării Bunurilor, prețul Contractului în termenele și modalitatea stabilite de Contract.

1. Obiectul Contractului

1.1. Vanzătorul își asumă obligația de a livra Bunurile conform Specificației tehnice din **Anexa nr.1** și Specificația de preț din **Anexa nr.2** care este parte integrantă a prezentului Contract.

1.2. Cumpărătorul se obligă, la rândul său, să achite și să recepționeze Bunurile livrate de către Vanzător.

1.3. Termenele de garanție a bunurilor livrate este de 12 luni.

2. Termeni și condiții de livrare

2.1. Livrarea Bunurilor se efectuează de către Vanzător Timp de 90 zile din data înaintării comunicării către Vanzător privind transmiterea dării de seamă la Agenția Achiziții Publice, cu livrare și descărcare a bunurilor la depozitul CNAS din str. Gheorghe Tudor nr. 3 mun. Chișinău, cu recepționarea de către persoana responsabilă desemnată din cadrul CNAS.

2.2. Documentația de însoțire a Bunurilor include:

1) Originalele facturilor fiscale2 ex

2) Actul de predare-primire **Anexa nr.3** 2 ex.

2.3. Originalele documentelor prevăzute în punctul 2.2 se vor prezenta Cumpărătorului cel târziu la momentul livrării bunurilor la destinația finală. Livrarea bunurilor se consideră încheiată în momentul în care sunt prezentate documentele de mai sus.

3. Prețul și condițiile de plată

3.1. Prețul Bunurilor livrate conform prezentului Contract, este stabilit în lei moldovenești, fiind indicat în Specificația prezentului Contract.

3.2. Suma totală a prezentului Contract, inclusiv TVA, se stabilește în lei moldovenești și constituie: _____ lei MD.

(suma cu cifre și litere)

3.3. Metoda și condițiile de plată de către Cumpărător vor fi: *Achitarea va fi efectuată după livrare, prin*

transfer, pe contul Vânzătorului, timp de 15 zile din data livrării bunurilor și semnării facturii fiscale.

3.4 Plățile se vor efectua prin transfer bancar pe contul de decontare al Vânzătorului indicat în prezentul Contract.

4. Condiții de predare-primire

4.1. Bunurile se consideră predate de către Vânzător și recepționate de către Cumpărător dacă:

- a) cantitatea Bunurilor corespunde specificației tehnice **Anexa nr.1**, specificației de preț **Anexa nr.2** și informației indicate în documentele de însoțire conform punctului 2.2 al prezentului Contract;
- b) calitatea Bunurilor corespunde informației indicate în specificația tehnică **Anexa nr.1** și în Partea II "Condițiile speciale ale contractului";

4.2. Vânzătorul este obligat să prezinte Cumpărătorului un exemplar original al facturii fiscale odată cu livrarea Bunurilor, pentru efectuarea plății. Pentru nerespectarea de către Vânzător a prezentei clauze, Cumpărătorul își rezervă dreptul de a majora termenul de achitare prevăzut în punctul 3.3 corespunzător numărului de zile de întârziere și de a fi exonerat de achitarea penalității stabilite în punctul 10.3.

5. Standarde

5.1. Bunurile livrate în baza contractului vor respecta standardele și normativele de domeniu sau alte reglementări autorizate.

6. Obligațiile părților

6.1. În baza prezentului Contract, Vânzătorul se obligă:

- a) să livreze Bunurile în condițiile prevăzute în specificația tehnică din **Anexa nr.1**.
- b) să anunțe Cumpărătorul, după semnarea prezentului Contract, în decurs de __5__ zile calendaristice, prin telefon/fax sau poșta electronică achizitiicnas@cnas.gov.md, despre disponibilitatea livrării Bunurilor;
- c) să asigure condițiile corespunzătoare pentru recepționarea Bunurilor de către Cumpărător, în termenele stabilite, în corespundere cu cerințele prezentului Contract;
- d) să asigure integritatea și calitatea Bunurilor pe toată perioada de până la recepționarea lor de către Cumpărător.

6.2. În baza prezentului Contract, Cumpărătorul se obligă:

- a) să întreprindă toate măsurile necesare pentru asigurarea recepționării în termenul stabilit a Bunurilor livrate în corespundere cu cerințele prezentului Contract;
- b) să asigure achitarea Bunurilor livrate, respectând modalitățile și termenele indicate în prezentul Contract.

7. Circumstanțe care justifică neexecutarea contractului

7.1. Părțile sunt exonerate de răspundere pentru neîndeplinirea parțială sau integrală a obligațiilor conform prezentului Contract, dacă aceasta este cauzată de producerea unor cazuri de circumstanțe care justifică neexecutarea contractului (războaie, calamități naturale: incendii, inundații, cutremure de pământ, precum și alte circumstanțe care nu depind de voința Părților).

7.2. Partea care invocă clauza circumstanțelor care justifică neexecutarea contractului este obligată să informeze imediat (dar nu mai târziu de 10 zile) cealaltă Parte despre survenirea circumstanțelor care justifică neexecutarea contractului.

7.3. Survenirea circumstanțelor care justifică neexecutarea contractului, momentul declanșării și termenul de acțiune trebuie să fie confirmate printr-un aviz de atestare, eliberat în mod corespunzător de către organul competent din țara Părții care invocă asemenea circumstanțe.

7.4. În cazul în care, în circumstanțele care justifică neexecutarea contractului, acesta se modifică prin acord adițional, inclusiv modificarea termenilor de executare, în cazul unei executări ulterioare a contractului. Când se execută pct.7.1 și pct. 7.3, părțile modifică contractul prin acord adițional, privind neîndeplinirea parțială sau integrală a obligațiilor, inclusiv modificarea termenilor în cazul suspendării și executării ulterioare a contractului.

8. Rezoluțiunea

- 8.1. Rezoluțiunea Contractului se poate realiza cu acordul comun al Părților.
- 8.2. Contractul poate fi rezolvit în mod unilateral de către:
- a) Cumpărător, în caz de refuz al Vanzătorului de a livra Bunurile prevăzute în prezentul Contract;
 - b) Cumpărător, în caz de nerespectare de către Vanzător a termenelor de livrare stabilite;
 - c) Vanzător, în caz de nerespectare de către Cumpărător a termenelor de plată a Bunurilor;
 - d) Vanzător sau Cumpărător, în caz de nesatisfacere de către una dintre Părți a pretențiilor înaintate conform prezentului Contract.
- 8.3. Cumpărătorul are dreptul de a rezolvi unilateral contractul în perioada de valabilitate a acestuia în una dintre următoarele situații:
- a) contractantul se afla, la momentul atribuirii lui, în una dintre situațiile care ar fi determinat excluderea sa din procedura de atribuire potrivit art. 19 al Legii nr.131/2015 privind achizițiile publice;
 - b) contractul a făcut obiectul unei modificări substanțiale care necesită o nouă procedură de achiziție publică în conformitate cu art. 76 al Legii nr.131/2015 privind achizițiile publice;
 - c) contractul nu ar fi trebuit să fie atribuit contractantului respectiv, având în vedere o încălcare gravă a obligațiilor ce rezultă din Legea nr.131/2015 privind achizițiile publice și/sau tratatele internaționale la care Republica Moldova este parte, care a fost constatată printr-o decizie a unei instanțe judecătorești naționale sau, după caz, internaționale.
- 8.4. Partea inițiatoare a rezoluțiunii Contractului este obligată să comunice, în termen de 5 zile lucrătoare, celeilalte Părți despre intențiile ei printr-o scrisoare motivată.
- 8.5. Partea înștiințată este obligată să răspundă în decurs de 5 zile lucrătoare de la primirea notificării. În cazul în care litigiul nu este soluționat în termenele stabilite, partea inițiatoare va iniția rezoluțiunea.

9. Reclamații

- 9.1. Reclamațiile privind cantitatea Bunurilor livrate sunt înaintate Vanzătorului la momentul recepționării lor, fiind confirmate printr-un act întocmit în comun cu reprezentantul Vanzătorului.
- 9.2. Pretențiile privind calitatea bunurilor livrate sunt înaintate Vanzătorului în termen de 5 zile de la depistarea deficiențelor de calitate și trebuie confirmate printr-un certificat eliberat de o organizație independentă, neutră și autorizată în acest sens.
- 9.3. Vanzătorul este obligat să examineze pretențiile înaintate în termen de 3 zile de la data primirii acestora și să comunice Cumpărătorului despre decizia luată.
- 9.4. În caz de recunoaștere a pretențiilor, Vanzătorul este obligat, în termen de 5 zile, să livreze suplimentar Cumpărătorului cantitatea nelivrată de bunuri, iar în caz de constatare a calității necorespunzătoare – să le substituie sau să le corecteze în conformitate cu cerințele Contractului.
- 9.5. Vanzătorul poartă răspundere pentru calitatea Bunurilor în limitele stabilite, inclusiv pentru viciile ascunse.
- 9.6. În cazul devierii de la calitatea confirmată prin certificatul de calitate întocmit de organizația independentă, neutră sau autorizată în acest sens, cheltuielile pentru staționare sau întârziere sunt suportate de către partea vinovată.

10. Sancțiuni

- 10.1. Pentru refuzul de a vinde Bunurile prevăzute în prezentul Contract, Vanzătorului i se va reține o penalitate în valoare de 5% din suma totală a contractului.
- 10.2. Pentru livrarea cu întârziere a Bunurilor, Vanzătorul poartă plata despăgubirii în valoare de 0,1% din suma Bunurilor nelivrate, pentru fiecare zi de întârziere, dar nu mai mult de 5% din suma totală a prezentului Contract. În cazul în care întârzierea depășește 15 zile, se consideră ca fiind refuz de a livra Bunurile prevăzute în prezentul Contract și Vanzătorului i se va reține o penalitate în valoare de 5% din suma totală a contractului în conformitate cu prevederile pct.10.1.
- 10.3. Pentru achitarea cu întârziere, Cumpărătorul poartă plata despăgubirii în valoare de 0,1% din suma Bunurilor neachitate, pentru fiecare zi de întârziere, dar nu mai mult de 5% din suma totală a

prezentului contract.

10.4. Prima zi lucrătoare ulterioară datei ce constituie termenul limită de livrare, precum și, termenul limită de achitare se consideră zi lucrătoare de întârziere.

10.5. Suma penalității calculate Vânzătorului conform prezentului Contract poate fi dedusă (reținută) de către Cumpărător din suma plății pentru Bunurile livrate.

11. Drepturi de proprietate intelectuală

11.1. Vânzătorul are obligația să despăgubească Cumpărătorul împotriva oricărui:

a) reclamații și acțiuni în justiție, care rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), legate de echipamentele, materialele, instalațiile sau utilajele folosite pentru sau în legătură cu produsele achiziționate, și

b) daune-interese, costuri, taxe și cheltuieli de orice natură, aferente, cu excepția situației în care o astfel de încălcare rezultă din respectarea Caietului de sarcini întocmit de către Cumpărător.

12. Dispoziții finale

12.1. Litigiile care ar putea rezulta din prezentul Contract vor fi soluționate de către Părți pe cale amiabilă. În caz contrar, ele vor fi transmise spre examinare în instanța de judecată competentă conform legislației Republicii Moldova.

12.2. Părțile contractante au dreptul, pe durata îndeplinirii contractului, să convină asupra modificării clauzelor contractului prin acord adițional, numai în cazul apariției unor circumstanțe care lezează interesele comerciale legitime ale acestora și care nu au putut fi prevăzute la data încheierii contractului. Modificările și completările la prezentul Contract sunt valabile numai în cazul în care au fost perfectate în scris și au fost semnate de către ambele Părți.

12.3. Nici una dintre Părți nu are dreptul să transmită obligațiile și drepturile sale stipulate în prezentul Contract unor terțe persoane fără acordul în scris al celeilalte părți.

12.4. Prezentul Contract, în cazul în care este semnat electronic de către ambele părți, este remis în mod automat prin mijloacele electronice, iar în cazul când contractul este semnat olografic, se întocmește în două exemplare, în limba română, câte un exemplar pentru Vânzător și pentru Cumpărător.

12.5. Prezentul Contract este întocmit în două exemplare în limba de stat a Republicii Moldova, câte un exemplar pentru Vânzător și pentru Cumpărător, se consideră încheiat la data semnării și intră în vigoare din data comunicării către Vânzător privind transmiterea către Agenția de Achiziții Publice a dării de seamă.

12.6. Prezentul contract este valabil până la **31.12.2026**.

12.8. Pentru confirmarea celor menționate mai sus, Părțile au semnat prezentul Contract în conformitate cu legislația Republicii Moldova.

II. CONDIȚIILE SPECIALE ALE CONTRACTULUI

1. Cerințe suplimentare:

1. Echipamentul propus trebuie să fie furnizat de producători recunoscuți mondiali (BRAND NAME).
2. Furnizorul va asigura instalarea și configurarea echipamentului prin specialiștii certificați menționați în ofertă, în ferestre de mentenanță agreeate, fără întreruperea serviciilor critice.
3. Garanția echipamentelor livrate cade în răspunderea vânzătorului pe toată perioada de garanție definită în ofertă.
4. În cazul apariției unor defecțiuni în perioada de garanție, furnizorul are obligația de a efectua reparațiile necesare sau de a asigura înlocuirea elementelor defecte cu piese de rezervă conforme, pe propria cheltuială. Deservirea în cazul unor neajunsuri sau defectări tehnice a utilajului are loc conform programului de lucru de către furnizor la Aparatul Central CNAS. Recepționarea și livrarea utilajului reparat în baza garanției se efectuează la sediul Aparatului

- Central CNAS.
5. Bunurile vor fi livrate cu transportul Vânzătorului și descărcate în depozitul aparatului central CNAS mun. Chișinău, str. Gheorghe Tudor 3.
 6. Bunurile livrate urmează să fie însoțite de certificatul de origine și certificatul de atestare a calității echipamentului.
 7. Bunurile livrate trebuie să fie noi, nefolosite și ne-recondiționate (non-refurbished) și să nu fie fabricate cu mai mult de 12 luni înainte de data livrării.

RECHIZITELE JURIDICE, POȘTALE ȘI DE PLATĂ ALE PĂRȚILOR

Vânzătorul

Adresa poștală:

Telefon:

Banca:

Cod Bancar:

IBAN:

Cod fiscal:

Cumpărătorul

Casa Națională de Asigurări Sociale

Adresa poștală: mun. Chișinău, str. Gh. Tudor, №3

Telefon: (022)25-75-51

Ministerul Finanțelor, Trezoreria de Stat

Cod Bancar: TREZMD2X

IBAN: MD84TRPFAH518710AO1691AA

Cod fiscal: 1004600030235

SEMNĂTURILE PĂRȚILOR

“Vânzător”:

L.Ș.

“Cumpărător”:

Directoare generală Elena ȚÎBÎRNĂ

L.Ș.

SPECIFICAȚII TEHNICE –

Denumire bunurilor solicitate	Specificarea tehnică deplină solicitată, Standarde de referință	Cantitatea
1.	<u>Echipamente de rețea de tip Next Generation Firewall (NGFW)</u> <u>Cerințe tehnice</u> 1. Protecția rețelei cu controlul stării sesiunilor; 2. Recunoașterea și blocarea aplicațiilor de rețea la nivelul 7 al modelului OSI în funcție de traficul care trece prin firewall, inclusiv individual pentru toate aplicațiile care folosesc porturi comune, inclusiv 80 și 443, precum și pentru aplicațiile care utilizează porturi TCP/UDP dinamice; 3. Firewall-ul NGFW propus trebuie să fie certificat minim conform standardelor ISO 27001, ISO 27017, ISO 27018, ISO 27701, Germany C5, Common Criteria, FIPS 140-2, CMVP. 4. Firewall-ul NGFW propus nu trebuie să necesite o repornire pentru a verifica și instala actualizările de securitate. 5. Firewall-ul NGFW propus trebuie să poată identifica aplicațiile indiferent de portul utilizat, criptarea SSL/SSH sau metodele de ocolire folosite. 6. Firewall-ul NGFW propus trebuie să clasifice aplicațiile neidentificate pentru gestionarea politicii, analiza criminalistică a amenințărilor sau dezvoltarea tehnologiilor de identificare a aplicațiilor. 7. Firewall-ul NGFW propus trebuie să fie o soluție dezvoltată inițial pentru asigurarea securității (nu un management de aplicații cu un firewall de bază care verifică starea). 8. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas. 9. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas. 10. Firewall-ul NGFW propus trebuie să poată să delimiteze diferite părți ale unei aplicații, cum ar fi permiterea chat-ului pe Facebook, dar blocarea posibilității de a trimite fișiere. 11. Firewall-ul NGFW propus trebuie să controleze accesul și să aplice politici pentru site-uri web și aplicații, inclusiv pentru aplicațiile SaaS. 12. Firewall-ul NGFW propus trebuie să utilizeze un sistem de operare unificat în toate formatele. 13. Firewall-ul NGFW propus trebuie să sprijine crearea politicii de securitate pentru prevenirea furtului de credențiale. 14. Firewall-ul NGFW propus trebuie să sprijine aplicarea autentificării multi-factor pentru aplicațiile interne. 15. Firewall-ul NGFW propus trebuie să permită vizibilitatea și controlul aplicațiilor care folosesc porturi non-standard, într-o politică unică de securitate. 16. Firewall-ul NGFW propus trebuie să poată oferi algoritmi de învățare	10 bucăți

	automată pentru protecție avansată direct din NGFW, fără a necesita conexiuni externe. 17. Recunoașterea în traficul inspectat la Layer-7 al modelului OSI a semnăturilor stocate pe MFE pentru următoarele categorii de aplicații: 17.1 . Aplicații corporative: 17.1.1. Servicii de autentificare, inclusiv Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS; 17.1.2. Sisteme de gestionare a bazelor de date (SGBD), inclusiv Microsoft SQL, Oracle, DB2, Postgres, Sybase; 17.1.3. Servicii de fișiere, inclusiv Microsoft SMB. 17.1.4. ERP, CRM, inclusiv SAP, 1C; 17.1.5. Sisteme de management al documentelor electronice și schimb de mesaje, inclusiv EMC Documentum, Microsoft SharePoint, Exchange, Lync, Office 365, Google Docs, Lotus; 17.1.6. Protocoale de schimb de e-mail: SMTP, POP3, IMAP; 17.1.7. Protocoale VoIP și conferințe audio-video, inclusiv SIP, H.323, H.245, H.225, Webex; 17.1.8. Servicii de actualizare software, inclusiv Microsoft Update, software antivirus (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple; 17.1.9. Servicii de backup, inclusiv Symantec Backup Exec; 17.1.10. Servicii de virtualizare și acces la terminale, inclusiv VMware, Citrix, Microsoft RDP; 17.1.11. Alte protocoale și tehnologii utilizate pentru crearea aplicațiilor distribuite, inclusiv CORBA, SOAP; 17.1.12. Protocoale de acces de la distanță, inclusiv Telnet, SSH, VNC, Radmin; 17.1.13. Protocoale de rețea, inclusiv protocoale de rutare dinamică și SSL, IPsec VPN; 17.2. Aplicații Internet: 17.2.1. E-mail, inclusiv Gmail, Yandex.Mail, Mail.ru, Hotmail; 17.2.2. Rețele sociale, inclusiv Facebook, Google+, LinkedIn, ВКонтакте, Odnoklassniki, „Moy Mir”; 17.2.3. Servicii de mesagerie instantanee, inclusiv Jabber, IRC, MSN, servicii similare în cadrul rețelelor sociale enumerate mai sus; 17.2.4. Servicii de conferință audio-video 17.2.5. Servicii de schimb de fișiere prin HTTP(S) și peer-to-peer, inclusiv Dropbox, BitTorrent, eMule, Google Drive, Yandex Disk, Gnutella, Boxnet, WebDav; 17.2.6. Streaming audio-video (indiferent de site-ul web), inclusiv YouTube, Vimeo, audio și video prin HTTP; 17.2.7. Servicii de publicare a desktop-ului și oferirea de acces de la distanță, inclusiv TeamViewer, LogMeIn; 17.2.8. Proxy externe și anonimizatoare, inclusiv Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy; 17.2.9. Servicii de construire a VPN-urilor private și tuneluri deasupra altor aplicații, inclusiv FreeNet, Open-VPN, VTun, RDP-to-TCP, TCP-over-DNS; 18. Oferirea de instrumente integrate în MFE pentru crearea semnăturilor proprii de aplicații bazate pe expresii regulate folosind decodare pentru HTTP(S), FTP, SMB, SMTP, RPC și altele, precum și pe mască pentru conținutul pachetelor TCP/UDP;	
--	--	--

	19. Recunoașterea aplicațiilor transmise prin protocolul HTTP/2; 20. Recunoașterea aplicațiilor de rețea prin traficul criptat SSL (suport pentru chei RSA de până la 2048 de biți) și SSHv2 care trece prin firewall (decriptarea SSL, SSHv2) – atât pentru conexiunile intrante, cât și pentru cele ieșite, transparent pentru utilizatori în domeniu, cu posibilitatea de a controla funcțiile individuale ale aplicațiilor, inclusiv trimiterea de mesaje pe rețelele sociale, schimbul de fișiere, streaming audio și video; 21. Inspecția tunelurilor: 21.1. Generic Routing Encapsulation (GRE) (RFC 2784); 21.2. Trafic IPsec necriptat [NULL Encryption Algorithm pentru IPsec (RFC 2410)]; 21.3. Mod de transport AH IPsec. 22. Recunoașterea secvențială a diferitelor aplicații utilizate într-o singură sesiune; 23. Recunoașterea utilizatorilor care folosesc aplicații de rețea prin integrarea cu serviciile corporative de autentificare a utilizatorilor, cum ar fi Microsoft Active Directory, Microsoft Exchange, Novell eDirectory, LDAP, Citrix; posibilitatea integrării cu alte servicii de autentificare (de exemplu, controlerele de rețea wireless) printr-o API XML deschisă; posibilitatea de a utiliza autentificarea forțată a utilizatorilor folosind o pagină WEB – „Captive portal”; suport pentru Kerberos, Tacacs+, SAML v.2, suport pentru roaming-ul L3 al utilizatorilor prin sondaje WMI și NetBios; 24. Inspecția în timp real a conținutului traficului transmis prin firewall pe baza semnăturilor și comportamentului, protecția împotriva vulnerabilităților, atacurilor de rețea și a malware-ului, recunoașterea tipurilor de fișiere pe baza semnăturilor acestora, detectarea virușilor transmiși prin web, e-mail, FTP, SMB, spyware, viermi de rețea, blocarea transmiterii unor conținuturi specifice folosind expresii regulate, inclusiv pentru aplicațiile care utilizează criptare SSL și SSHv2; 25. Crearea de reguli pentru traficul care trece prin firewall într-o politică unificată de securitate, utilizând următorii parametri pentru fiecare conexiune: 25.1. Adresa IP a expeditorului, 25.2. Adresa IP a destinatarului, 25.3. Serviciile L4 utilizate: porturi pentru protocoalele TCP și UDP, 25.4. Numele utilizatorilor sau grupurilor de utilizatori din Active Directory, 25.5. Aplicațiile la nivelul 7 al modelului OSI, 25.6. URL categorii. 26. Crearea de reguli într-o politică unificată de securitate, utilizând ca parametri informațiile despre adresele IP ale expeditorului, destinatarului, serviciile utilizate (porturi TCP/UDP), numele utilizatorilor, grupurilor de utilizatori și aplicațiile utilizate de aceștia sau anumite categorii de aplicații. În politicile create, trebuie să existe posibilitatea implementării următoarelor acțiuni: • Permisivitate sau interdicție; • Permisivitatea unui anumit aplicații sau categorii de aplicații de a utiliza doar porturi TCP/UDP standard sau strict definite. Aceste porturi nu trebuie să fie folosite de alte aplicații fără o politică care să permită	
--	--	--

	explicit astfel de interacțiuni; • Permisiiune, dar cu scanare pentru viruși și alte amenințări; • Permisiiune sau interdicție pe bază de orar, utilizator sau grup de utilizatori; • Decriptare și verificare. Dacă nu s-a putut decripta (în cazul unui algoritm criptografic nestandard, certificat expirat etc.) – interdicere; • Ne-decriptarea anumitor categorii de URL și site-uri web de încredere; • Aplicarea marcajului DSCP și limitarea traficului folosind politici QoS bazate pe aplicații, adrese IP, utilizatori și grupuri de utilizatori; • Implementarea hardware a QoS pentru traficul real-time, identificat la nivelul aplicațiilor; • Aplicarea redirectionării traficului pe bază de politici (Policy Based Forwarding); • Permisiiunea anumitor funcții ale aplicației; • Oricare combinație dintre acțiunile de mai sus. 27. Protecție antivirus, protecție împotriva software-ului spyware, protecție împotriva vulnerabilităților și atacurilor de rețea (sistem de detecție și prevenire a intruziunilor), filtrare URL utilizând o bază dinamică de reputație, care susține categorizarea diferitelor secțiuni ale aceleiași site web, inclusiv susținerea categoriilor pentru site-uri web în limba rusă, blocarea transferului de fișiere pe baza tipurilor definite de semnături; 28. Posibilitatea de a verifica suplimentar traficul pentru amenințări necunoscute prin analiza acestuia utilizând tehnologia învățării automate prin servicii cloud; 29. Detectarea și filtrarea solicitărilor către resursele din rețea în funcție de categoria acestora, de exemplu, site-uri malware, rețele sociale, resurse publicitare etc.; 30. Suport pentru acțiuni: permisiune, notificare, blocare, solicitarea confirmării utilizatorului, solicitarea parolei utilizatorului; 31. Filtrarea URL trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 32. Analiza SNI în TLS Hello simultan cu URL-ul în cererea HTTP pentru a contracara tehnicile de ocolire de tip SNIcat; 33. Analiza cererilor DNS suspecte, domeniilor DGA și localizarea stațiilor infectate utilizând tehnologia DNS sinkhole (modificarea răspunsului serverului DNS); 34. Detectarea tehnicilor de ocolire a protecției prin cereri DNS care încearcă să folosească domenii generate automat (DGA), inclusiv analiza frecvenței n-gramelor, analiza entropiei, frecvența cererilor, tunelarea în DNS, canale de transfer de date prin cereri DNS, inclusiv tuneluri DNS ultra-lente; 35. Blocarea domeniilor DGA, domeniilor DGA create pe baza unui dicționar, tehnici de ocolire DNS-rebinding, FastFlux, interogări către înregistrări DNS suspendate, atacuri NSNX, atacuri cu domenii recent înregistrate; 36. Analiza cererilor DNS suspecte trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 37. Protecție împotriva tehnicilor de evitare (evasions), de exemplu MPTCP; 38. Oferirea unui serviciu de scanare a fișierelor potențial dăunătoare necunoscute în sandbox cu sisteme de operare Microsoft Windows, Linux prin metoda de emulare a rulării și vizualizare a documentelor;	
--	--	--

	39. Sandbox-ul trebuie să verifice fișierele executabile suspecte (inclusiv EXE, DLL, SCR, BAT, etc.), fișiere ELF, documente în formatele PDF, MS Office 2007, 2010, 2016 și mai sus, Java și Flash, Android APK, Mach-O, DMG și PKG, arhive RAR, ZIP, 7Zip; 40. Firewall-ul trebuie să trimită spre verificare în sandbox fișierele suspecte transmise prin aplicațiile HTTP, SMTP, POP3, IMAP, SMB, FTP, precum și implementările acestora prin SSL, dacă există; 41. Sandbox-ul trebuie să genereze și să trimită către firewall un raport despre verificarea fișierului; 42. Sandbox-ul trebuie să genereze semnături pentru blocarea atacurilor de tip zero-day pentru utilizarea pe toate firewall-urile companiei în aplicațiile enumerate, în decurs de 5 minute de la primirea fișierului pentru verificare; 43. Firewall-ul trebuie să primească semnăturile fișierelor din sandbox și să aibă un motor de blocare bazat pe noile semnături obținute de la sandbox-ul cloud sau local; 44. Sandbox-ul furnizorului cloud trebuie să aibă posibilitatea de a schimba semnături între toți clienții furnizorului; 45. Firewall-ul trebuie să primească din sandbox indicatori de compromitere: IP, URL, DNS, care sunt utilizate de codul malițios și să blocheze conexiunile pe baza listei de indicatori malițioși. 46. Sandbox-ul trebuie să verifice linkurile HTTP:// și HTTPS:// din e-mailuri prin protocoalele SMTP/POP3. 47. Sandbox-ul trebuie să verifice fișierele din aplicațiile criptate SSL, cel puțin în protocolul HTTPS. 48. Suport obligatoriu pentru învățarea automată în timpul inspectării amenințărilor de tip zero-day pentru a reduce întârzierea în inspecția fișierelor suspecte; 49. Sandbox-ul trebuie să asigure analiza comportamentului fișierelor și linkurilor suspecte în cloud privat sau extern (sandbox), să detecteze noi malware și să genereze automat semnături antivirus în decurs de 5 minute și să actualizeze baza de reputație URL în decurs de 30 de minute, care se vor instala pe toate dispozitivele Clientului cu abonamentele corespunzătoare; 50. Posibilitatea integrării cu subsistemul de detectare a amenințărilor zero-day, implementat pe un dispozitiv hardware dedicat aceluiași furnizor, plasat pe obiectul central al Clientului (cloud privat), care permite generarea automată a semnăturii antivirus local, pe dispozitivul hardware dedicat în centrul de date (DC) al Clientului în decurs de 5 minute; 51. Sandbox-ul local dedicat trebuie să aibă un API pentru primirea fișierelor spre verificare atât de la firewall-uri, cât și de la servicii terțe; 52. Sandbox-ul trebuie să genereze rapoarte despre verificările efectuate și să permită vizualizarea acestora în format PDF; 53. Sandbox-ul cloud trebuie să utilizeze tehnologia Bare Metal Analysis fără a utiliza emularea sistemului de operare; 54. Firewall-ul trebuie să aibă capacitatea de a trimite fișiere diferite în sandbox-uri diferite, de exemplu, fișierele EXE în sandbox-ul cloud, iar fișierele DOC în sandbox-ul local; 55. Sandbox-ul cloud trebuie să accepte fișiere PE pentru verificare, chiar și în absența unui abonament; 56. Suport pentru următorii furnizori de autentificare multi-factor (Multi-	
--	---	--

	Factor Authentication - MFA) (direct, fără utilizarea produselor intermediare): Duo, • Okta, • RSA SecureID, • PingID; 57. Protecție împotriva furtului de loginuri și parole ale utilizatorilor prin integrarea cu Active Directory (AD), monitorizarea transmiterii conturilor de utilizator către zone de securitate neîncredere, autentificarea forțată a utilizatorilor prin autentificare cu doi factori (MFA); 58. Funcționalitate de control granular al accesului utilizatorilor de la distanță în mediul de lucru corporativ, cu posibilitatea de verificare a existenței anumitor software-uri pe stația de lucru a utilizatorului și accesul prin dispozitive mobile; 59. Funcționalitate de protecție împotriva atacurilor DoS; 60. Posibilitatea de a activa 100% din semnăturile IPS, antivirus, filtrarea URL-urilor, controlul aplicațiilor și Threat Intelligence fără a degrada performanța; 61. Funcționalitate de blocare a scanării porturilor ICMP/TCP/UDP; 62. Detectarea obiectelor din fișierele transmise prin rețea care conțin informații importante și blocarea transmiterii acestor fișiere; 63. Detectarea prezenței datelor filtrabile în fișierele transmise prin rețea, incluzând, dar fără a se limita la: Adobe PDF, HTML, Microsoft Office (Excel, Word, PowerPoint). Rich Text Format; 64. Prezența șabloanelor de date preconfigurate, cum ar fi numerele de carduri de credit. 65. Suport pentru crearea de șabloane proprii de date pe baza expresiilor regulate. 66. Posibilitatea de integrare cu subsistemul de management centralizat, logare, raportare și actualizare a software-ului pentru firewall-uri de același furnizor. 67. Cerințe pentru sistemul de management centralizat: • Funcționalități avansate de vizualizare a activității aplicațiilor rețelei, amenințărilor rețelei detectate și blocate, utilizarea aplicațiilor de către utilizatori. Permite filtrarea informațiilor pe aplicații, amenințări, utilizatori, adrese IP, porturi TCP/UDP, zone de securitate, tipuri de amenințări etc.; • Corelarea automată a jurnalelor de diferite tipuri, generate în cadrul aceleiași sesiuni (filtrarea traficului prin firewall, protecția împotriva amenințărilor, controlul transferului de fișiere, filtrarea URL); • Posibilitatea de corelare automată a evenimentelor de securitate folosind obiecte de corelare actualizabile care folosesc informații de la protecția antivirus, protecția împotriva software-ului spyware, protecția împotriva vulnerabilităților și atacurilor, amenințările de tip zero-day; • Funcționalități de generare automată a rapoartelor și de generare a rapoartelor pe bază de program, cu opțiuni de personalizare manuală a rapoartelor. Rapoartele trebuie să fie vizibile prin interfața grafică (GUI) și să poată fi exportate în formate PDF și CSV. • Posibilitatea de a configura funcționalitățile SD-WAN prin consola de management centralizat. • Sistemul trebuie să poată exporta logurile către soluții externe prin	
--	--	--

	syslog, utilizând formate standardizate precum CEF sau LEEF; • Trebuie să existe mecanisme de inițializare automată pentru echipamente noi, inclusiv în locații la distanță, fără intervenție manuală; • Trebuie să fie posibilă actualizarea centralizată a software-ului pentru echipamentele administrate, într-un mod simplificat; • Soluția trebuie să ofere interfețe moderne de integrare (REST API) compatibile cu XML și JSON, pentru interoperabilitate cu alte sisteme. • Fiecare administrator trebuie să poată face modificări izolate, cu salvare separată, pentru a evita suprascrierea neintenționată; • Sistemul trebuie să permită definirea de roluri și permisiuni personalizate pentru utilizatori, cu acces diferențiat la funcționalități. • Platforma trebuie să permită organizarea echipamentelor și configurațiilor prin grupuri, ierarhii și etichete; • Sistemul trebuie să suporte funcționare în mod redundant (high availability) și echilibrare a sarcinii (load balancing); 68. Posibilitatea de a detecta și analiza traficul dispozitivelor IoT folosind algoritmi de învățare automată. 69. Funcționalitatea de a trimite traficul SSL decriptat către dispozitive externe. 70. Funcționalitatea de a captura traficul de la dispozitive externe și de a-l cripta într-un tunel SSL pentru transmiterea prin Internet. 71. Prezența unui raport separat pentru aplicațiile de tip SaaS. 72. Funcționalitatea IPSec VPN. 73. Integrarea cu sistemele externe SIEM/SIM prin protocolul Syslog, cu configurare flexibilă a formatului jurnalelor. 74. Suport pentru rutare statică și protocoale de rutare dinamică BGP, OSPF, RIP. 75. Suport pentru diverse moduri de lucru ale interfețelor rețelei (monitorizare trafic mirroring, mod transparent, Layer 2 și Layer 3). 76. Suport pentru IPv6, inclusiv identificarea aplicațiilor și utilizatorilor. 77. Suport pentru multicast, incluzând PIM-SM, PIM-SSM, IGMP v1, v2, v3. 78. Suport pentru rutarea între VLAN-uri. 79. Suport pentru NAT, DHCP și DHCP relay. 80. Suport pentru etichetarea cadrelor prin 802.1Q (minim 4094 VLAN-uri). 81. Suport pentru agregarea interfețelor prin 802.3ad (suport LACP). 82. Suport pentru pachete mari (Jumbo frames). 83. Managementul rolurilor administratorilor locali: • Posibilitatea de a restricționa vizualizarea și gestionarea la nivelul dispozitivului și al sistemelor virtuale (contexte); • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la orice secțiune a interfeței web; • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la CLI-ul firewall-ului. 84. Firewall-ul hardware trebuie să dispună de o platformă hardware specializată, care să permită administrarea dispozitivului fără întreruperi, chiar și în condiții de încărcare maximă. Trebuie să fie asigurate resurse de procesare dedicate, separate pentru analiza	
--	--	--

	traficului monitorizat și pentru activitățile de management. Administrarea fiecărui dispozitiv în parte trebuie să se realizeze prin protocoalele HTTPS și SSH, fără a necesita instalarea vreunui software suplimentar de administrare pe stația de lucru a administratorului. Interfața de administrare a firewall-urilor (web și CLI) trebuie să fie unificată cu subsistemul de management centralizat, jurnalizare, raportare și actualizare a software-ului. Cerințe de performanță ale firewall-ului: Performance: • Threat prevention throughput 1.2 Gbps; • IPsec VPN throughput 800 Mbps; • Connections per second 1100; • Firewall throughput 1.4 Gbps; Policies: • Security rules min 500; • Security rule schedules min 256; • NAT rules min 400; • Tunnel content inspection rules 100; • SD-WAN rules min 100; • Policy based forwarding rules min 100; • DoS protection rules min 100. Security Zones: • security zones 25. Security Profiles: • Security profiles min 75. URL Filtering: • Total entries for allow list, block list and custom categories 25,000; Interfaces: • I/O: 1G RJ45 (7); • Management I/O: 10/100/1000 out-of-band management port (1), RJ45 console port (1), USB port (1). Storage Capacity: • 128 GB Virtual Routers: • Virtual routers 3. Routing: • IPv4 forwarding table size min 5,000; • IPv6 forwarding table size min 2500; • System total forwarding table size min 5,000; L2 Forwarding: • ARP table size per device 1500; • IPv6 neighbor table size 1500; • MAC table size per device 1500; Address Assignment: • DHCP servers 3; • DHCP relays 500; • IPSec VPN:	
--	---	--

	• Suport Site to site over gre IPSec tunnels • SD-WAN IPsec tunnels 85. Alte cerințe obligatorii: - Garanție, Mentenanta si Suport HW+SW incluse – 12 luni; - Producătorul trebuie să ofere suport prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului; - Ofertantul va indica în ofertă costul serviciilor pentru efectuarea instalării și configurării a echipamentului oferat, va asigura integrarea echipamentului oferat cu dispozitivele existente pe baza platformei existente in cadrul instituției prin realizarea configurărilor necesare, cu setarea tuturor parametrilor aplicabili în corespundere cu cerințele înaintate pe infrastructura Beneficiarului. - Prezentarea a certificatelor a minim 1 specialist pe produsul oferat din partea ofertantului (fără asociere cu o alta companie); - Ofertantul va prezenta copia Certificatului ISO 27001:2018, in domeniul serviciilor privind asigurarea securității informației, design-ul acestuia, implementarea, monitorizarea si managementul infrastructurii IT - Ofertantul va prezenta Certificatului ISO 9001:2015, pentru Servicii de comercializare și implementare suport tehnic în garanție și post garanție pentru sisteme informaționale, echipamente hardware si software și Servicii privind asigurarea securității informației, designul, implementarea, monitorizarea si managementul infrastructurii IT si de Securitate – certificat confirmat cu aplicarea semnăturii electronice; - Ofertantul va prezenta Autorizarea de la producător pentru licitația la care participa; - Ofertantul va avea minim o persoana certificata in calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013; - Referințe de vânzare NGFW – minim 3 contracte; - Termen de livrare: maxim pana la 90 zile de la data intrării în vigoare a contractului	
--	---	--

SEMNĂTURILE PĂRȚILOR

Vânzătorul

L.Ș.

Cumpărătorul
Directoare generală Elena ȚÎBÎRNĂ

L.Ș.

Anexa nr. 2

la contractul nr. _____
din “ ____ ” _____ 2026

SPECIFICAȚII DE PREȚ -

Nr	Specificarea tehnică deplină solicitată	Cantitate bucăți	Preț unitar fără TVA	Preț unitar cu TVA	Suma fără TVA	Suma cu TVA
1	<u>Echipamente de rețea de tip Next Generation Firewall (NGFW)</u>	10				
Suma totală fără TVA lei MD						
Suma totală cu TVA lei MD						

SEMNĂTURILE PĂRȚILOR

Vânzătorul

Cumpărătorul
Directoare generală Elena ȚÎBÎRNĂ

L.Ș.

L.Ș.

Anexa nr. 3

la contractul nr. _____
din “ _____ ” _____ 2026

Model de act de primire predare

ACT de primire-predare

Prin prezentul act se confirmă transmiterea bunurilor prevăzute de contractul Nr. _____ din
” _____ ” _____ 2026.

Se confirmă faptul că **agentul economic** _____
a transmis bunul

(descifrarea serviciilor și pieselor, cu indicarea prețurilor)

în cantitatea _____ la data de _____ 2026.

Vânzător _____

Cumpărător _____

SEMNĂTURILE PĂRȚILOR

Vânzător

Cumpărător

Directoare generală Dna Elena ȚÎBÎRNĂ

L.Ș.

L.Ș.