

DOCUMENTAȚIA STANDARD

pentru realizarea achizițiilor publice de bunuri prin cererea ofertelor de prețuri

Obiectul achiziției: *Pachet software antivirus (prelungirea licențelor)*

Cod CPV: **48761000-0**

Autoritatea Contractantă: *I.P. "Centrul de Tehnologii Informationale în Finante",
Cod Fiscal 1005600036924,
MD-2005, Republica Moldova,
mun. Chișinău, str. Constantin Tănase, 7,
Tel: 022 262 873, e-mail: ctif@ctif.gov.md*

CAPITOLUL I
INSTRUCȚIUNI PENTRU OFERTANȚI (IPO)
[Notă: nu se va modifica de către Autoritatea Contractantă]

Secțiunea 1. Dispoziții generale

1. Scopul procedurii de achiziție

1.1. Autoritatea contractantă, emite Documentele de atribuire în vederea achiziționării de bunuri/servicii, după cum este specificat în Fișa de Date a Achiziției (în continuare **FDA**).

2. Principiile care stau la baza atribuirii contractului de achiziție

2.1. Principiile care stau la baza atribuirii contractului de achiziție publică sînt:

- a) libera concurență;
- b) eficiența utilizării fondurilor publice și minimizarea riscurilor autorităților/entițailor contractante;
- c) transparența;
- d) tratamentul egal, imparțial și nediscriminatoriu în privința tuturor ofertanților și operatorilor economici;
- e) protecția mediului;
- f) respectarea ordinii de drept;
- g) confidențialitatea;
- h) asumarea răspunderii în cadrul procedurilor de achiziție publică.

3. Sursa de finanțare

3.1. În **FDA** va fi specificată sursa de finanțare pentru plățile contractului ce urmează a fi atribuit.

3.2. Autoritatea contractantă urmează să se asigure că la momentul inițierii procedurii de achiziții publice, mijloacele financiare sunt alocate și destinate exclusiv achiziției în cauză.

3.3. În cazul lipsei mijloacelor financiare, **FDA** va conține argumentarea justificativă a autorității contractante privind alocarea ulterioară pentru procedura de achiziție curentă.

4. Participanții la procedura de achiziție

4.1. Participant la procedura de achiziție poate fi orice operator economic rezident sau nerezident, persoană fizică sau juridică de drept public sau privat ori asociație de astfel de persoane, care are dreptul de a participa, în condițiile Legii nr. 131/2015 privind achizițiile publice (în continuare Legea nr. 131/2015), la procedura de atribuire a contractului de achiziții publice.

4.2. Dreptul de participare la procedurile de atribuire a contractelor de achiziții publice poate fi rezervat de către Guvern unor ateliere protejate și întreprinderi sociale de inserție în cazul în care majoritatea angajaților implicați sînt persoane cu dizabilități care, prin natura sau gravitatea deficiențelor lor, nu pot desfășura o activitate profesională în condiții normale.

5. Cheltuielile de participare la procedura de achiziție

5.1. Ofertantul suportă toate costurile legate de pregătirea și înaintarea ofertei, iar autoritatea contractantă nu poartă nici o responsabilitate pentru aceste costuri, indiferent de desfășurarea sau rezultatul procedurii de achiziție.

5.2. La depunerea ofertelor, operatorul economic, după caz, va achita o taxă. Modul de achitare a taxei menționate, precum și cuantumul acesteia sînt stabilite de Guvern.

5.3. Achitarea taxei pentru depunerea ofertei se va efectua prin intermediul platformei de achiziții electronice prin care se depune oferta.

6. Limba de comunicare în cadrul procedurii de achiziție

6.1. Oferta, Documentul Unic de Achiziții European (în continuare **DUAE**), documentele de atribuire și toată corespondența dintre ofertant și autoritatea contractantă vor fi întocmite în limba de stat. Documentele justificative și literatura de specialitate tipărită, care fac parte din ofertă, pot fi în altă limbă, cu condiția ca acestea să fie însoțite de o traducere exactă a fragmentelor relevante în limba de stat.

6.2. Autoritatea contractantă poate specifica după caz, în **FDA** posibilitatea depunerii ofertei și într-o altă limbă de circulație internațională.

7. Secțiunile Documentelor de atribuire

7.1. Documentele de atribuire includ toate secțiunile indicate în prezentul punct și trebuie citite în conjuncție cu orice modificare conform punctului IPO8.

CAPITOLUL I. Instrucțiuni pentru ofertanți

CAPITOLUL II. Fișa de date a achiziției

CAPITOLUL III. Formulare pentru depunerea ofertei

CAPITOLUL IV. Specificații tehnice și de preț.

CAPITOLUL V. Formularul de contract

8. Clarificarea și modificarea documentelor de atribuire

8.1. Participantul poate solicita clarificări asupra documentelor de atribuire prin intermediul SIA „RSAP”, iar autoritatea contractantă va răspunde la rîndul său prin același mijloc, la orice cerere de clarificare, înainte de termenul-limită pentru depunerea ofertelor.

8.2. Pînă la expirarea termenului de depunere a ofertelor, autoritatea contractantă are dreptul să modifice documentația de atribuire fie din proprie inițiativă, fie ca răspuns la solicitarea de clarificare a unui operator economic, prelungind, după caz, termenul de depunere a ofertelor, astfel încît de la data aducerii la cunoștință a modificărilor operate pînă la noul termen de depunere a ofertelor să rămîna cel puțin 50% din termenul stabilit inițial.

8.3. În cazul în care operatorul economic nu a transmis solicitarea de clarificare în timp util, punînd astfel autoritatea contractantă în imposibilitate de a respecta termenele prevăzute la art. 34, alin. (4) din Legea nr. 131/2015, aceasta din urmă este în drept să nu răspundă.

9. Practicile de corupere și alte practici interzise

9.1. Autoritățile contractante și participanții la procedurile de achiziții publice vor respecta cele mai înalte standarde ale eticii de conduită în desfășurarea și implementarea proceselor de achiziții, precum și în executarea contractelor de achiziție publică.

9.2. În cazul în care autoritatea contractantă va depista că ofertantul a fost implicat în practicile menționate la punctul IPO9.4 în cadrul procesului de concurență pentru contractul de achiziție publică sau pe parcursul executării contractului, aceasta:

a. va exclude ofertantul din procedura respectivă de achiziție prin includerea lui în Lista de interdicție, conform prevederilor Regulamentului cu privire la Lista de interdicție a operatorilor economici; sau

b. va întreprinde orice alte măsuri prevăzute în articolul 40 al Legii nr. 131/2015.

9.3. În cazul în care, Agenția Achiziții Publice, în procesul de monitorizare a procedurilor de achiziții publice, constată că un operator economic a fost implicat în practicile menționate la punctul IPO9.4, va raporta imediat organelor competente fiecare caz de corupere sau de tentativă de corupere comis de operatorul economic respectiv.

9.4. În cadrul procedurilor de achiziție și executării contractului nu se permit următoarele acțiuni:

a. promisiunea, oferirea sau darea unei persoane cu funcție de răspundere, personal sau prin mijlocitor, de bunuri sau servicii, sau a oricărui alt lucru de valoare, pentru a influența acțiunile unei alte părți;

b. 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;

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

d. deteriorarea sau prejudicierea, direct sau indirect, a oricărei părți sau a proprietății acestei părți, pentru a influența în mod necorespunzător acțiunile acesteia;

e. distrugerea intenționată, falsificarea, contrafacerea sau ascunderea materialelor de evidență ale investigării, sau darea unor informații false anchetatorilor, pentru a împiedica esențial o anchetă condusă de către organele de resort în vederea identificării unor practici menționate la lit. a)-d); precum și amenințarea, hărțuirea sau intimidarea oricărei părți pentru a o împiedica să divulge informația cu privire la chestiuni relevante anchetei sau să exercite ancheta.

9.5. Personalul autorității contractante are obligația de a exclude practicile de corupere în vederea obținerii beneficiilor personale în legătură cu desfășurarea procedurii de achiziții publice.

Secțiunea a-2-a. Criterii de calificare

10. Criterii generale

10.1. Pentru confirmarea datelor de calificare în cadrul procedurii de achiziții publice, operatorul economic va completa și va prezenta **DUAE**, în conformitate cu cerințele stabilite de autoritatea contractantă.

10.2. Prezentarea oricărui alt formular **DUAE** decât cel solicitat de către autoritatea contractantă, va servi ca temei de descalificare de la procedura de achiziție publică.

10.3. Autoritatea contractantă va aplica criteriile și cerințele de calificare numai referitoare la:

- a) eligibilitatea ofertantului sau candidatului;
- b) capacitatea de exercitare a activității profesionale;
- c) capacitatea economică și financiară;
- d) capacitatea tehnică și/sau profesională;
- e) standarde de asigurare a calității;
- f) standarde de protecție a mediului.

11. Eligibilitatea ofertantului sau candidatului

11.1. Orice operator economic, rezident sau nerezident, persoană 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.

11.2. Va fi exclus 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

infraacțiuni legate de activități teroriste, finanțarea terorismului, exploatarea prin muncă a copiilor și alte forme de trafic de persoane.

11.3. Va fi exclus de la procedura pentru atribuire a contractului de achiziție publică, și respectiv nu este eligibil, orice ofertant care se află în oricare dintre următoarele situații:

- a. se află în proces de insolvență ca urmare a hotărârii judecătorești;
- b. nu și-a îndeplinit obligațiile de plată a impozitelor, taxelor și contribuțiilor de asigurări sociale către bugetele componente ale bugetului general consolidat, în conformitate cu prevederile legale în Republica Moldova sau în țara în care este stabilit;
- c. a fost condamnat, în ultimii trei ani, prin hotărârea definitivă a unei instanțe judecătorești, pentru o faptă care a adus atingere eticii profesionale sau pentru comiterea unei greșeli în materie profesională;
- d. prezintă informații false sau nu prezintă informațiile solicitate de către autoritatea contractantă, în scopul demonstrării îndeplinirii criteriilor de calificare și selecție;
- e. a încălcat obligațiile aplicabile în domeniul mediului, muncii și asigurărilor sociale, în cazul în care autoritatea contractantă demonstrează, prin orice mijloace adecvate, acest fapt;
- f. se face vinovat de o abatere profesională, care îi pune la îndoială integritatea, în cazul în care autoritatea contractantă demonstrează, prin orice mijloace adecvate, acest fapt;
- g. a încheiat cu alți operatori economici acorduri care vizează denaturarea concurenței, în cazul în care acest fapt se constată printr-o decizie a organului abilitat în acest sens;
- h. se află într-o situație de conflict de interese care nu poate fi remediată în mod efectiv prin măsurile prevăzute la art.74 din Legea nr. 131/2015;
- i. este inclus în Lista de interdicție a operatorilor economici.

11.4. Autoritatea contractantă, după caz, poate stabili în documentația de atribuire posibilitatea furnizării dovezilor de către operatorii economici care se află în una din situațiile menționate la punctele IPO11.2 și IPO11.3, prin care se vor prezenta măsurile luate de aceștia pentru a demonstra fiabilitatea sa, în pofida existenței unui motiv de excludere.

11.5. Autoritatea contractantă extrage informația necesară pentru constatarea existenței sau inexistenței circumstanțelor menționate la punctele IPO11.2 și IPO11.3 din 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 menționate la punctele IPO11.2 și IPO11.3 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.

11.6. În ceea ce privește cazurile menționate la punctul IPO11.3, în conformitate cu legislația internă a statului în care sunt stabiliți ofertanții, aceste solicitări se referă la persoane fizice și persoane 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.

11.7. 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 punctul IPO11.4 sau respectivele documente nu vizează toate situațiile prevăzute la punctele IPO11.2 și IPO11.3, 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.

11.8. Orice operator economic aflat în oricare dintre situațiile prevăzute la punctele IPO11.2 și IPO11.3 care atrag excluderea din procedura de atribuire poate furniza dovezi care să arate că măsurile luate de acesta sunt suficiente pentru a-și demonstra în concret credibilitatea prin raportare

la motivele de excludere, 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.

11.9. 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 sînt insuficiente, autoritatea contractantă informează ofertantul/candidatul despre motivele excluderii.

12. Capacitatea de exercitare a activității profesionale

12.1. Autoritatea contractantă poate solicita oricărui ofertant să prezinte dovada din care să rezulte o formă de înregistrare ca persoană juridică, capacitatea legală de a livra bunuri sau de a presta servicii, în conformitate cu prevederile legale din țara în care este stabilit

13. Capacitatea economică și financiară

13.1. În cazul în care autoritatea contractantă solicită demonstrarea capacității economice și financiare, aceasta are obligația de a indica în documentația de atribuire și informațiile pe care operatorii economici urmează să le prezinte în acest scop. Capacitatea economică și financiară se realizează, după caz, prin prezentarea unuia sau mai multor documente relevante, cum ar fi:

- a. declarații bancare corespunzătoare sau, după caz, dovezi privind asigurarea riscului profesional;
- b. rapoarte financiare sau, în cazul în care publicarea acestor rapoarte este prevăzută de legislația țării în care este stabilit ofertantul, extrase de rapoarte financiare;
- c. declarații privind cifra de afaceri totală sau, dacă este cazul, privind cifra de afaceri în domeniul de activitate aferent obiectului contractului într-o perioadă anterioară care vizează activitatea din ultimii 3 ani, în măsura în care informațiile respective sînt disponibile. În acest ultim caz, autoritatea contractantă are obligația de a lua în considerare și data la care operatorul economic a fost înființat sau și-a început activitatea comercială.

13.2. În sensul punctului IPO13.1 (literei c), cifra de afaceri anuală minimă impusă operatorilor economici nu trebuie să depășească de două ori valoarea estimată a contractului, cu excepția cazurilor justificate, precum cele legate de riscurile speciale aferente naturii bunurilor/serviciilor.

13.3. Atunci cînd un contract este împărțit în loturi, indicele cifrei de afaceri se aplică pentru fiecare lot individual. Cu toate acestea, autoritatea contractantă stabilește cifra de afaceri anuală minimă impusă operatorilor economici cu referire la grupuri de loturi, dacă ofertantului cîștigător îi sînt atribuite mai multe loturi care trebuie executate în același timp.

13.4. În cazul în care, din motive obiective, justificate corespunzător, operatorul economic nu are posibilitatea de a prezenta documentele solicitate de autoritatea contractantă, acesta are dreptul de a demonstra capacitatea sa economică și financiară prin prezentarea altor documente pe care autoritatea contractantă le poate considera edificatoare în măsura în care acestea reflectă o imagine fidelă a situației economice și financiare a ofertantului/candidatului.

13.5. Ofertantul/candidatul poate să-și demonstreze capacitatea economică și financiară și prin susținerea acordată de către o altă persoană indiferent de natura relațiilor juridice existente între ofertant/candidat și persoana respectivă.

13.6. În cazul prevăzut la punctul IPO13.5, ofertantul/candidatul 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, prin care această persoană confirmă faptul că va pune la dispoziția ofertantului/candidatului resursele financiare invocate.

13.7. Persoana care asigură susținerea financiară trebuie să îndeplinească criteriile de selecție relevante și nu trebuie să se afle în niciuna dintre situațiile prevăzute la punctul IPO11.2 și punctul IPO11.3 literele c)-g), care determină excluderea din procedura de atribuire.

13.8. O asociație de operatori economici la fel are dreptul să se bazeze pe capacitățile membrilor asociației sau ale altor persoane.

14. Capacitate tehnică și/sau profesională

14.1. În cazul aplicării unei proceduri pentru atribuirea unui contract de achiziții publice de bunuri/servicii, în scopul verificării capacității tehnice și/sau profesionale a ofertanților/candidaților, autoritatea contractantă are dreptul de a le solicita acestora, în funcție de specificul, de volumul și de complexitatea bunurilor/serviciilor ce urmează să fie livrate/prestate și 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, următoarele:

a) lista principalelor bunuri/servicii similare livrate/prestate în ultimii 3 ani, conținînd valori, perioade de livrare/prestare, beneficiari, indiferent dacă aceștia din urmă sînt autorități contractante sau clienți privați. Livrarea de bunuri sau prestările de servicii se confirmă prin prezentarea unor certificate/documente emise sau contrasemnate de o autoritate ori de către clientul privat beneficiar. În cazul în care beneficiarul este un client privat și, din motive obiective, operatorul economic nu are posibilitatea obținerii unei certificări/confirmări din partea acestuia, demonstrarea furnizărilor de bunuri sau prestărilor de servicii se realizează printr-o declarație a operatorului economic;

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

c) 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;

d) informații referitoare la studiile, pregătirea profesională și calificarea personalului de conducere, precum și ale persoanelor responsabile pentru îndeplinirea contractului, dacă acestea nu reprezintă factori de evaluare stabiliți de autoritatea contractantă;

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

f) dacă este cazul, informații privind măsurile de protecție a mediului pe care operatorul economic le poate aplica în timpul îndeplinirii contractului;

g) informații referitoare la utilajele, instalațiile, echipamentele tehnice de care va dispune operatorul economic pentru îndeplinirea corespunzătoare a contractului;

h) informații privind partea din contract pe care operatorul economic are, eventual, intenția să o subcontracteze.

14.2. Capacitatea tehnică și profesională a ofertantului poate fi susținută, pentru îndeplinirea unui contract, și de o altă persoană, indiferent de natura relațiilor juridice existente între ofertant și persoana respectivă.

14.3. În cazul prevăzut la punctul IPO14.2, ofertantul/candidatul 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, prin care această persoană confirmă faptul că va pune la dispoziția ofertantului/candidatului resursele financiare invocate.

14.4. Persoana care asigură susținerea financiară trebuie să îndeplinească criteriile de selecție relevante și nu trebuie să se afle în niciuna dintre situațiile prevăzute la punctul IPO11.2 și punctul IPO11.3 literele c)-g), care determină excluderea din procedura de atribuire.

14.5. Ofertantul/candidatul are dreptul să recurgă la susținerea unor alte persoane doar atunci cînd acestea din urmă vor desfășura activitățile sau serviciile pentru îndeplinirea cărora este necesară capacitatea profesională respectivă.

15. Standarde de asigurare a calității.

15.1. Autoritatea contractantă solicită prezentarea unor certificate, emise de organisme independente, prin care se atestă faptul că operatorul economic respectă anumite standarde de asigurare a calității, aceasta 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.

15.2. 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.

16. Standarde de protecție a mediului.

16.1. Autoritatea contractantă solicită prezentarea unor certificate, emise de organisme independente, prin care se atestă faptul că operatorul economic respectă anumite standarde de protecție a mediului, aceasta trebuie să se raporteze:

- a) fie la Sistemul Comunitar de Management de Mediu și Audit (EMAS);
- b) fie la standarde de gestiune ecologică bazate pe seriile de standarde europene sau internaționale în domeniu, certificate de organisme conforme cu legislația Uniunii Europene ori cu standardele europene sau internaționale privind certificarea.

16.2. 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.

17. Calificarea candidaților în cazul asocierii

17.1. În cazul unei asocieri, cerințele solicitate pentru îndeplinirea criteriilor de calificare și selecție referitoare la capacitatea de exercitare a activității profesionale și cele referitoare la eligibilitatea ofertantului sau candidatului, trebuie îndeplinite de către fiecare asociat. Criteriile referitoare la situația economică și financiară și cele referitoare la capacitatea tehnică și profesională pot fi îndeplinite prin cumul proporțional sarcinilor ce revin fiecărui asociat. Criteriile privind cifra de afaceri, în cazul unei asocieri, cifra de afaceri medie anuală luată în considerare va fi valoarea generală, rezultată prin însumarea cifrelor de afaceri medii anuale corespunzătoare fiecărui membru al asocierii. În cazul unei asocieri, cerințele privind standardele de asigurare a calității și standardele de protecție a mediului, trebuie îndeplinite de fiecare membru al asocierii.

Secțiunea a-3-a. Pregătirea ofertelor

18. Documentele ce constituie oferta

18.1. Oferta va cuprinde următoarele:

- a) Oferta de prețuri, care va include, după caz, și garanția pentru ofertă;
- b) Specificația tehnică pentru bunurile/serviciile achiziționate;
- c) Documentul unic de achiziții european;

18.2. Operatorii economici vor pregăti ofertele într-o manieră structurată și securizată, ca răspuns la anunțul de participare publicat de către autoritatea contractantă în SIA „RSAP” și vor depune ofertele în mod electronic, folosind fluxurile interactive de lucru puse la dispoziție de

platformele electronice, cu excepția cazurilor prevăzute la art.32 alin.(7) și (11) din Legea nr. 131/2015.

19. Documente pentru demonstrarea conformității bunurilor/serviciilor

19.1. Pentru a stabili conformitatea bunurilor/serviciilor cu cerințele documentelor de atribuire, ofertantul desemnat câștigător la procedura de achiziție în cauză, va prezenta, la solicitarea autorității contractante, dovezi documentare ce atestă faptul că bunurile/serviciile se conformează condițiilor de livrare/prestare, specificațiilor tehnice și standardelor specificate în CAPITOLUL IV.

19.2. Pentru a demonstra conformitatea tehnică a bunurilor/serviciilor propuse, cantităților propuse și a termenelor de livrare/prestare, ofertantul va completa Formularul Specificații tehnice (**F4.1**) și Specificații de preț (**F4.2**). De asemenea, ofertantul va include documentație de specialitate, desene, extrase din cataloage și alte date tehnice justificative, după caz.

20. Oferte alternative

20.1. Operatorul economic este în drept să depună oferte alternative numai în cazul în care autoritatea contractantă a precizat explicit în anunțul de participare și în **FDA** punctul **3.1** că permite sau solicită depunerea de oferte alternative cu precizarea în documentația de atribuire a cerințelor minime obligatorii pe care operatorii economici trebuie să le respecte, precum și orice alte cerințe specifice pentru prezentarea ofertelor alternative. În cazul în care în documentația de atribuire nu este specificat explicit că autoritatea contractantă permite sau solicită depunerea de oferte alternative, aceasta din urmă nu are dreptul de a lua în considerare ofertele alternative.

21. Garanția pentru ofertă

21.1. În cazul în care în **FDA** punctul **3.2** autoritatea contractantă indică necesitatea prezentării garanției pentru ofertă, ofertantul va depune, ca parte a ofertei sale, o Garanție pentru ofertă (**F3.2**).

21.2. Garanția pentru ofertă va fi corespunzător cuantumului specificat în **FDA** punctul **3.3**, în lei moldovenești, și va fi:

- a) în formă de garanție bancară de la o instituție bancară licențiată, valabilă pentru perioada de valabilitate a ofertei sau altă perioadă prelungită, după caz, în conformitate cu punctul IPO23.2; sau
- b) transfer pe contul autorității contractante; sau
- c) alte forme acceptate de autoritatea contractantă, specificate în **FDA** punctul **3.2**.

21.3. Dacă o garanție pentru ofertă este cerută în conformitate cu punctul IPO21.2, orice ofertă neînsoțită de o astfel de garanție pregătită în modul corespunzător va fi respinsă de către autoritatea contractantă ca fiind necorespunzătoare.

21.4. Garanția pentru ofertă a ofertanților necâștigători va fi restituită imediat de la producerea oricărui din următoarele evenimente:

- a) expirarea termenului de valabilitate a garanției pentru ofertă;
- b) încheierea unui contract de achiziții publice și depunerea garanției de bună execuție a contractului, dacă o astfel de garanție este prevăzută în documentația de atribuire;
- c) suspendarea procedurii de achiziție fără încheierea unui contract de achiziții publice;
- d) retragerea ofertei înainte de expirarea termenului de depunere a ofertelor, în cazul în care documentația de atribuire nu prevede inadmisibilitatea unei astfel de retrageri.

21.5. Garanția pentru ofertă va fi reținută dacă:

a) ofertantul își retrage sau își modifică oferta în timpul perioadei de valabilitate a ofertei specificate de către ofertant în Formularul ofertei, cu excepția cazurilor prevăzute în punctul IPO23.2; sau

b) ofertantul câștigător refuză:

- să deponă Garanția de bună execuție conform punctului IPO42;
- să semneze contractul conform punctului IPO43.

21.6. Garanția pentru ofertă prezentată de Asociație trebuie să fie în numele Asociației care depune oferta.

22. Prețuri

22.1. Prețurile indicate de către ofertant în Formularul ofertei (**F3.1**) și în Specificațiile de preț (**F4.2**) se vor conforma cerințelor specificate în punctul IPO22.

22.2. Toate loturile și pozițiile trebuie enumerate și evaluate separat în Specificațiile tehnice (**F4.1**) și Specificațiile de preț (**F4.2**).

22.3. Prețul ce urmează a fi specificat în Formularul ofertei va constitui suma totală a ofertei, inclusiv TVA.

22.4. Termenii Incoterms, cum ar fi EXW, CIP, DDP și alți termeni similari, vor fi supuși regulilor prevăzute în ediția curentă a Incoterms, publicată de către Camera Internațională de Comerț, după cum este menționat în **FDA** punctul **3.4**.

22.5. Prețurile vor fi indicate după cum este arătat în Specificațiile de preț (**F4.2**).

22.6. Autoritatea contractantă va efectua achitări conform metodologiei și condițiilor indicate în **FDA** punctul **3.7**.

23. Termenul de valabilitate a ofertelor

23.1. Ofertele vor rămâne valabile pe parcursul perioadei specificate în **FDA** punctul **3.8**, de la data-limită de depunere a ofertei stabilită de autoritatea contractantă. O ofertă valabilă pentru un termen mai scurt va fi respinsă de către autoritatea contractantă ca fiind necorespunzătoare.

23.2. În cazuri excepționale, înainte de expirarea perioadei de valabilitate a ofertei, autoritatea contractantă poate solicita ofertanților să extindă perioada de valabilitate a ofertelor. Solicitarea și răspunsul la solicitarea de prelungire a valabilității ofertei vor fi publicate în SIA „RSAP”. În cazul în care se cere o garanție pentru ofertă în cadrul procedurii de achiziție publică, conform prevederilor punctului IPO23, operatorul economic va extinde corespunzător valabilitatea garanției pentru ofertă. Un ofertant poate refuza solicitarea de extindere fără a pierde garanția pentru ofertă. Ofertanților ce acceptă solicitarea de extindere nu li se va cere și nu li se va permite să modifice ofertele.

24. Valuta ofertei

24.1. Prețurile pentru bunurile/serviciile solicitate vor fi indicate în lei moldovenești, cu excepția cazurilor în care **FDA** punctul **3.9**, prevede altfel.

25. Formatul ofertei

25.1. Oferta va fi pregătită în format electronic, în conformitate cu cerințele autorității contractante, cu ajutorul instrumentelor existente în SIA „RSAP”, cu excepția cazurilor prevăzute la art.32 alin.(7) și (11) din Legea nr. 131/2015.

Secțiunea a-4-a. Depunerea și deschiderea ofertelor

26. Depunerea ofertelor

26.1. Oferta , scrisă și semnată, se prezintă în format electronic în conformitate cu cerințele expuse în documentația de atribuire, utilizând SIA „RSAP”, cu excepția cazurilor prevăzute la art.32 alin.(7) și (11) din Legea nr. 131/2015. Autoritatea contractantă eliberează operatorului economic, în mod obligatoriu, o recipisă în care indică data și ora recepționării ofertei sau confirmă recepționarea acesteia în cazurile în care oferta a fost depusă prin mijloace electronice. Prezentarea ofertei presupune depunerea într-un set comun a ofertei de prețuri, a specificației tehnice, a **DUAE** și a garanției pentru ofertă după caz.

26.2. La depunerea ofertei prin SIA „RSAP”, operatorul economic va ține cont de timpul necesar pentru încărcarea ofertei în sistem, prevăzând timp suficient pentru a depune oferta în termenii stabiliți.

27. Termenul limită de depunere a ofertelor

27.1. Ofertele vor fi depuse nu mai târziu de data și ora specificate în **FDA** punctul **4.2**. Autoritatea contractantă poate, la discreția sa, să extindă termenul-limită de depunere a ofertelor prin modificarea documentelor de atribuire în conformitate cu punctul IPO7.

28. Oferte întârziate

28.1. SIA „RSAP” nu va accepta ofertele transmise după expirarea termenului limită de depunere a ofertelor.

28.2. În cazurile prevăzute la art.32 alin.(7) și (11) din Legea nr. 131/2015, ofertele depuse după termenul limită de deschidere a ofertelor specificate în **FDA** punctul **4.2**, vor fi înregistrate de către autoritatea contractantă și restituite ofertantului, fără a fi deschise.

29. Modificarea, substituirea și retragerea ofertelor

29.1. În cazul în care documentația de atribuire nu prevede altfel, 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. O astfel de modificare este valabilă dacă a fost efectuată înainte de expirarea termenului de depunere a ofertelor.

30. Deschiderea ofertelor

30.1. Autoritatea contractantă va deschide ofertele în cadrul sistemului SIA „RSAP” la data și ora specificate în **FDA** punctul **4.2**.

30.2. Informația privind ofertanții și ofertele, se fac publice prin publicarea acestora în SIA „RSAP”.

Secțiunea a-5-a. Licitația electronică

30.3. Atribuirea unui contract de achiziții publice pentru bunuri și servicii prin cererea ofertelor de prețuri este obligatoriu precedată de licitația electronică

30.4. Licitația electronică se va baza pe una dintre următoarele elemente ale ofertei:

- a) exclusiv pe preț, în cazul în care contractul este atribuit doar în baza criteriului cel mai scăzut preț;
- b) pe preț și pe noile valori ale elementelor ofertelor indicate în anunțul de participare și/sau în documentația de atribuire.

30.5. În cazul în care procedura de achiziție de bunuri și servicii prin cererea ofertelor de prețuri este împărțită în loturi, licitația electronică se petrece pentru fiecare lot în parte.

30.6. Licitarea electronică se lansează la data și ora indicată în comunicatul expediat ofertanților pentru înregistrare la licitația electronică, cu condiția că cel puțin 2 operatori economici au depus ofertele în cadrul procedurii de achiziție. După lansare, licitația electronică nu poate fi suspendată sau anulată.

30.7. În cazul în care a fost depusă o singură ofertă, licitația electronică nu are loc, iar autoritatea contractantă urmează să decidă asupra atribuirii contractului de achiziții sau anularea procedurii de achiziție.

30.8. În timpul licitației electronice, ofertantul poate:

- a) să vizualizeze în timp real desfășurarea licitației electronice;
- b) să ofere o valoare nouă a ofertei în cadrul fiecărei runde de licitare.

30.9. Pe parcursul licitației electronice SIA RSAP va afișa identificatorul licitației electronice, tipul licitației electronice utilizate, valuta ofertelor, instrucțiunile pentru participanți, cea mai bună ofertă curentă, timpul rămas până la sfârșitul runde și clasamentul actual al operatorilor economici enumerați fără specificarea denumirii participantului.

30.10. În cadrul licitației electronice, la afișarea valorii ofertelor sistemul va lua în considerare toate elementele ofertei care fac obiectul procesului repetitiv de ofertare.

30.11. Licitarea electronică va lua sfârșit atunci când numărul de runde prevăzut în anunțul de participare și în documentația de atribuire a fost epuizat. Din momentul încheierii licitației electronice, SIA RSAP va publica rezultatul licitației electronice și numele participanților.

30.12. Referitor la prețul final, rezultat în urma licitației electronice, nu se mai pot solicita clarificări decât cu privire la justificarea prețului anormal de scăzut oferat, fără a se permite însă modificarea acestuia.

Secțiunea a-6-a. Evaluarea și compararea ofertelor

31. Confidențialitate

31.1. SIA „RSAP” va asigura mecanisme adecvate în vederea neadmiterii divulgării conținutului ofertelor prezentate de participanți până la data stabilită pentru deschiderea acestora de către persoanele autorizate ale organizatorului procedurii de achiziție publică, în conformitate cu legislația. Astfel, va fi preîntâmpinată aplicarea unor eventuale practici anticoncurențiale în cadrul procedurilor de achiziții publice.

32. Clarificarea ofertelor

32.1. Autoritatea contractantă poate, la necesitate, să ceară oricărui dintre ofertanți o clarificare a ofertei acestora, pentru a facilita examinarea, evaluarea și compararea ofertelor. Nu vor fi solicitate, oferite sau permise schimbări în prețurile sau în conținutul ofertei, cu excepția corectării erorilor aritmetice descoperite de către autoritatea contractantă în timpul evaluării ofertelor, în conformitate cu punctul IPO33.

32.2. În cazul în care ofertantul nu execută cererea autorității contractante de a reconfirma datele de calificare pentru încheierea contractului, oferta i se respinge și se selectează o altă ofertă câștigătoare dintre ofertele rămase în vigoare.

32.3. Operatorul economic este obligat să răspundă la solicitarea de clarificare a autorității contractante în cel mult trei zile de la data expedierii acesteia.

33. Determinarea conformității ofertelor

33.1. Aprecierea corespunderii unei oferte de către autoritatea contractantă urmează a fi bazată pe conținutul ofertei.

33.2. Se consideră conformă cerințelor oferta care corespunde tuturor termenilor, condițiilor și specificațiilor din documentele de atribuire, neavând abateri esențiale sau având doar abateri neînsemnate, erori sau omiteri ce pot fi înlăturate fără a afecta esența ofertei. O abatere se va considera ca fiind neînsemnată dacă:

- a) nu afectează în orice mod substanțial sfera de acțiune, calitatea sau performanța bunurilor/serviciilor specificate în contract;
- b) nu limitează în orice mod substanțial drepturile autorității contractante sau obligațiile ofertantului conform contractului;
- c) nu ar afecta într-un mod inechitabil poziția competitivă a altor ofertanți ce prezintă oferte conforme cerințelor.

33.3. Dacă o ofertă nu este conformă cerințelor din documentele de atribuire, ea va fi respinsă de către autoritatea contractantă prin specificarea expresă a motivelor respingerii.

34. Neconformități, erori și omiteri

34.1. Autoritatea contractantă are dreptul să considere oferta conformă cerințelor dacă aceasta conține abateri neînsemnate de la prevederile documentelor de atribuire, erori sau omiteri ce pot fi înlăturate fără a afecta esența ei. Orice deviere de acest fel se va exprima cantitativ, în măsura în care este posibil, și se va lua în considerare la evaluarea și compararea ofertelor.

34.2. Dacă ofertantul care a depus oferta cea mai avantajoasă nu acceptă corectarea erorilor aritmetice, oferta acestuia se respinge.

35. Evaluarea ofertelor

35.1. Examinarea, evaluarea și compararea ofertelor se efectuează fără participarea ofertanților și a altor persoane neautorizate. Autoritatea contractantă va examina ofertele pentru a confirma faptul că toate documentele prevăzute în punctul IPO18 au fost prezentate și pentru a determina caracterul complet al fiecărui document depus.

35.2. Autoritatea contractantă stabilește oferta/ofertele câștigătoare aplicând criteriul de atribuire și factorii de evaluare prevăzuți în documentația de atribuire, utilizând instrumentele de evaluare din cadrul SIA „RSAP”, cu excepția cazurilor prevăzute la art.32 alin.(7) și (11) din Legea nr. 131/2015.

36. Calificarea ofertantului

36.1. Autoritatea contractantă va determina dacă ofertantul este calificat să execute Contractul.

36.2. Aprecierea calificării va fi bazată pe o examinare minuțioasă a documentelor de calificare ale ofertantului, inclusiv DUAЕ, incluse în ofertă conform prevederilor punctului IPO18, clarificărilor posibile conform punctului IPO32, precum și în baza criteriilor stabilite în punctele IPO11-16. Criteriile care nu au fost incluse în aceste puncte nu vor fi folosite în aprecierea calificării ofertantului.

36.3. O apreciere afirmativă va constitui drept premisă pentru adjudecarea contractului ofertantului respectiv. O apreciere negativă va rezulta în descalificarea ofertei, caz în care autoritatea contractantă poate trece la următoarea ofertă cea mai avantajoasă economic, pentru a face o apreciere similară a capacităților aceluși ofertant în executarea contractului.

37. Descalificarea ofertantului

37.1. Autoritatea contractantă va descalifica 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 poate înainta o solicitare către Agenția Achiziții Publice cu privire la înscrierea ofertantului respectiv în Lista de interdicție a operatorilor economici.

37.2. Lista de interdicție a operatorilor economici reprezintă un înscris oficial și este întocmită actualizată și ținută de către Agenția Achiziții Publice conform prevederilor articolului 25 din Legea nr. 131/2015, cu scopul de a limita participarea operatorilor economici la procedurile de achiziție publică

37.3. Ofertantul poate fi descalificat în cazul în care este insolubil, în privința lui a fost inițiată procedura de sechestrare a patrimoniului, este în faliment sau în proces de lichidare sau dacă activitățile ofertantului sînt suspendate ori există un proces de judecată privind oricare dintre cele menționate.

37.4. Ofertantul este descalificat în cazul aplicării sancțiunilor administrative sau penale, pe parcursul ultimilor 3 ani, față de persoanele de conducere ale operatorului economic în legătură cu activitatea lor profesională sau cu prezentarea de date eronate în scopul încheierii contractului de achiziții publice.

37.5. Ofertantul este descalificat pentru neachitarea impozitelor și altor plăți obligatorii în conformitate cu legislația țării în care el este rezident. Autoritatea contractantă va solicita ofertanților să demonstreze împuternicirea de a încheia contractele de achiziții publice și componența fondatorilor și a persoanelor afiliate.

37.6. Autoritatea contractantă descalifică ofertantul dacă constată că acesta este inclus în Lista de interdicție a operatorilor economici.

37.7. Autoritatea contractantă nu acceptă oferta în cazul în care ofertantul nu corespunde cerințelor de calificare.

38. Anularea procedurii

38.1. Autoritatea contractantă, din propria inițiativă, anulează procedura de achiziție publică în cazurile prevăzute la art. 67, alin. (1) din Legea nr. 131/2015. Autoritatea contractantă are obligația de a comunica prin SIA „RSAP” sau prin alte mijloace de comunicare în cazul în care autoritatea contractantă desfășoară proceduri în baza art. 32 alin.(7) și (11) din Legea nr. 131/2015, tuturor participanților la procedura de achiziție publică, în cel mult 3 zile de la data anulării, atît încetarea obligațiilor pe care aceștia și le-au creat prin depunerea de oferte, cît și motivul anulării.

Secțiunea a-7-a. Adjudecarea contractului

39. Criteriul de adjudecare

39.1. Autoritatea contractantă va adjudeca contractul, conform criteriului stabilit în **FDA** punctul **6.1**, aceluși ofertant a cărui ofertă a fost apreciată potrivit criteriilor stabilite precum și altor condiții și cerințelor din documentele de atribuire, cu condiția ca și ofertantul să fie calificat pentru executarea contractului.

40. Dreptul autorității contractante de a modifica cantitățile în timpul adjudecării

40.1. La momentul adjudecării contractului, autoritatea contractantă are posibilitatea de a micșora cu acordul operatorului economic, cantitatea de bunuri/servicii, în cazul în care suma contractelor este mai mare decît valoare estimată a achiziției, specificate inițial în CAPITOLUL IV pentru a se putea încadra în mijloacele financiare alocate, însă fără a efectua vreo schimbare în prețul unitar sau în alți termeni și condiții ale ofertei și ale documentelor de atribuire.

41. Înștiințarea de adjudecare

41.1. Înainte de expirarea perioadei de valabilitate a ofertei, sistemul SIA „RSAP” va permite autorităților contractante pregătirea anunțului de atribuire și a notificării ofertanților, cărora li s-a atribuit sau nu contractul standardizat. Ofertanții necâștigători vor fi informați cu privire la motivele pentru care ofertele lor nu au fost selectate.

41.2. Notificarea prin care se realizează informarea operatorilor economici referitor la rezultatele procedurii de achiziție este transmisă prin SIA „RSAP” sau prin alte mijloace electronice la adresele indicate de către ofertanți în ofertele acestora.

42. Garanția de bună execuție

42.1. La momentul încheierii contractului, dar nu mai târziu de data expirării Garanției pentru ofertă (dacă s-a cerut), ofertantul câștigător va prezenta Garanția de bună execuție în mărimea prevăzută de **FDA** punctul **6.2.**, folosind în acest scop formularul Garanției de bună execuție (**F3.3**), inclus în CAPITOLUL III, sau alt formular acceptabil pentru autoritatea contractantă, dar care corespunde condițiilor formularului (**F3.3**).

42.2. Refuzul ofertantului câștigător de a depune Garanția de bună execuție sau de a semna contractul va constitui motiv suficient pentru anularea adjudecării și reținerea Garanției pentru ofertă. În acest caz, autoritatea contractantă poate adjudeca contractul următorului ofertant cu oferta cea mai bine clasată, a cărei ofertă este conformă cerințelor și care este apreciat de către autoritatea contractantă a fi calificat în executarea Contractului. În acest caz, autoritatea contractantă va cere tuturor ofertanților rămași extinderea termenului de valabilitate a Garanției pentru ofertă. Totodată, autoritatea contractantă este în drept să respingă toate celelalte oferte.

43. Semnarea contractului

43.1. O dată cu expedierea înștiințării de adjudecare, autoritatea contractantă va trimite ofertantului câștigător Formularul contractului de bunuri (**F5.1**) sau Formularul contractului de servicii (**F5.2**) completat și toate celelalte documente componente ale contractului.

43.2. Ofertantul câștigător va semna contractul numai după împlinirea termenelor de așteptare, în modul corespunzător și îl va restitui autorității contractante în termenul specificat în **FDA** punctul **6.5**.

44. Dreptul de contestare

44.1. 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.

44.2. Contestățiile se vor depune direct la Agenția Națională de Soluționare a Contestățiilor. Toate contestațiile vor fi depuse, examinate și soluționate în modul stabilit de Legea nr. 131/2015.

44.3. Operatorul economic, în termen de până la 5 zile, sau după caz, 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 Contestățiilor o contestație argumentată a acțiunilor, a deciziei ori a procedurii aplicate de autoritatea contractantă.

44.4. Contestățiile privind anunțurile de participare la procedura de achiziție și documentația de atribuire vor fi depuse până la termenul limită de depunere a ofertelor.

CAPITOLUL II
FIȘA DE DATE A ACHIZIȚIEI (FDA)

Următoarele date specifice referitoare la bunurile/serviciile solicitate vor completa, suplimenta sau ajusta prevederile CAPITOLULUI I. În cazul unei discrepante sau al unui conflict, prevederile prezentului CAPITOL vor prevala asupra prevederilor din CAPITOLUL I.

1. Dispoziții generale

Nr.	Rubrica	Datele Autorității Contractante/Organizatorului procedurii
1.1.	Autoritatea contractantă/Organizatorul procedurii, IDNO:	<i>I.P. „Centrul de Tehnologii Informaționale în Finanțe” IDNO 1005600036924</i>
1.2.	Obiectul achiziției:	<i>Servicii de mentenanță a Sistemului Informațional de Evidență Contabilă 1C, Contabilitate versiune 8.3</i>
1.3.	Numărul procedurii de achiziție:	<i>Nr.: MTender ID ocds-b3wdp1-MD-1616657521500</i>
1.4.	Tipul obiectului de achiziție:	<i>Bunuri</i>
1.5.	Codul CPV:	<i>48761000-0</i>
1.6.	Sursa alocațiilor bugetare/banilor publici și perioada bugetară:	<i>Surse proprii, 2021</i>
1.7.	Administratorul alocațiilor bugetare:	<i>I.P. „Centrul de Tehnologii Informaționale în Finanțe”</i>
1.8.	Partenerul de dezvoltare (după caz):	<i>Nu se aplică</i>
1.9.	Denumirea cumpărătorului, IDNO:	<i>I.P. „Centrul de Tehnologii Informaționale în Finanțe” IDNO 1005600036924</i>
1.10.	Destinatarul bunurilor/serviciilor, IDNO:	<i>I.P. „Centrul de Tehnologii Informaționale în Finanțe” IDNO 1005600036924</i>
1.11.	Limba de comunicare:	<i>Limba de stat</i>
1.12.	Locul/Modalitatea de transmitere a clarificărilor referitor la documentația de atribuire	<i>Prin intermediul SIA „RSAP”</i>
1.13.	Contract de achiziție rezervat atelierelor protejate	<i>Nu se aplică</i>
1.14.	Tipul contractului:	<i>Vînzare-cumpărare</i>
1.15.	Condiții speciale de care depinde îndeplinirea contractului:	<i>Nu se aplică</i>

2. Lista bunurilor/serviciilor și specificațiile tehnice:

Nr. d/o	Cod CPV	Denumirea bunurilor	Unitatea de măsură	Cantitatea	Specificația tehnică deplină solicitată, Standarde de referință
1	48761000-0	Pachet software antivirus (prelungirea licențelor)	licențe	600	Conform specificației tehnice, din Anexa nr. 1

Anexa nr. 1

Specificațiile tehnice minime pentru sistemul de protecție și securitate cibernetică tip Antivirus

Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST) și să fie prezent în mențiunile Gartner. Satisfacerea necesităților minime va constitui: **500 licențe** (workstation PC, mailboxes), și **100 licențe** (VDI/VS/Server), în scopul managementului centralizat pentru dispozitive. **Licențele oferite trebuie să fie capabile să prelungească pe un termen de 12 luni, licențele existente compatibile sau echivalente pentru Bitdefender Gravity Zone Elite.**

Caracteristici generale ale produsului:

Produsul va conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management:

1. Protecție stații și servere fizice și virtualizate:
 - Windows 10,8.1,7, Vista (SP1), XP (SP3), Mac OS X 10.12.x, 10.11.x, 10.10.x, 10.9.x, 10.8.x
 - Windows Server 2003/2008/2008/2019 R2/2012/2012 R2/2016.
 - Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Oracle Linux 6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual, Debian 5.0 sau mai recent.
2. Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS și Android.
3. Protecție și securitate de tip „sandboxing” pentru serverele și stațiile de lucru;
4. Controlul dispozitivelor, controlul accesului la Internet, filtrarea traficului prin modul de tip firewall pentru mașinile fizice și virtuale
5. Protecție și securitate pentru serverele email Microsoft Exchange.

Consola de management:

Pachetul de instalare va fi oferit ca un appliance virtual. Aceasta din urmă nu va necesita o licență suplimentară pentru sistemul de operare, iar imaginea de tip template va fi posibil de a fi importată în următoarele platforme de virtualizare: VMware vSphere, Citrix XenServe, Microsoft Hyper-V, Red Hat Enterprise Virtualization, KVM, Oracle VM.

Consola de management va fi oferită cu o baza de date inclusă, non-relațională.

Soluția trebuie să:

1. Fie scalabilă, astfel ca oricare dintre roluri sau servicii să poată fi instalate separat sau împreună pe aceeași sau mai multe VDI-uri.
 2. Asigure următoarele roluri: server cu baza de date, server de comunicație, server de actualizare, server de web.
 3. Asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale VMware și Citrix prin task din consola de management.
 4. Includă un modul load balancer pentru performanța și redundanță
 5. Includă mecanisme de configurare a disponibilității pentru serverul cu baze de date (clustering).
 6. Includă posibilitatea de a fi accesată atât de pe stațiile de lucru cât și de pe dispozitivele mobile (tabletă, smartphone).
- Interfața consolei de management va fi în limba română. Interfața agentului care se instalează pe stații de lucru și servere, va fi în limba română.

Cerinte generale produs:

Soluția trebuie să:

1. Includă unul sau mai multe module de update server prin care să asigure actualizarea componentelor și a semnăturilor.
2. Permită activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management.
3. Transmite alerte de ne funcționalitate, cu 30 de minute înainte de actualizare.
4. Permită vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi și îmbunătățiri, probleme rezolvate, probleme cunoscute
5. Afișeze notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție viruși, actualizări de produs disponibile).
6. Permită integrarea cu un server Syslog pentru raportarea evenimentelor antivirus.
7. Permită instalarea serviciului de SNMP pentru raportarea statusului mașinilor din cadrul componentei de management.
8. Permită crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programat, stocată local, pe un server FTP sau în rețea

Inventarierea rețelei – managementul securității

Produsul trebuie să:

1. Se integreze cu domenii Active Directory multiple, VMware vCenter, Citrix Xen și să importe inventarul acestor platforme.
2. Permită descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.
3. Permită descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery.
4. Ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP.
5. Permită instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale.
6. Permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale.
7. Permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus.
8. Ofere posibilitatea de repornire a mașinilor fizice de la distanță.
9. Ofere informații detaliate despre fiecare task inițiat și afișarea statutului lui.

10. Permite configurarea centralizată a clienților antivirus prin intermediul politicilor.
11. Ofere în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături.
12. Permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea.
13. Permite crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux și Mac.

Politici:

Produsul trebuie să:

1. Permite configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module
2. Conțină opțiuni specifice de activare/dezactivare și configurare a funcționalităților precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user.
3. Permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directoy.
4. Poată fi schimbată automat în funcție de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este în accesai rețea cu infrastructura de management, Tipul rețelei (lan, wireless).

Monitorizare și raportare:

Produsul trebuie să:

1. Permite setarea de opțiuni specifice pentru afișarea rapoartelor existente.
2. Deține un panou central care să afișeze statutul modulelor și rapoartele lor pentru perioadele de timp specificate.
3. Conțină rapoarte care prezintă statusul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.
4. Trimită rapoarte către un număr nelimitat de adrese de email.
5. Permite vizualizarea rapoartelor curente programate de administrator.
6. Permite exportarea rapoartelor în format .pdf și detaliile ca format .csv.
7. Include un generator de rapoarte care să ofere posibilitatea de a investiga o problemă de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal, evenimente Exchange.
8. Ofere interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor.
9. Ofere interogări legate de evenimente precum: calculatorul ținta pe care a avut loc evenimentul, tipul starea și configurația agentului de securitate instalat, starea modulelor și rolurilor de protecție instalate pe agentul de securitate, denumirea și alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicații blocate, detecțiile etc)
10. Ofere interogări de evenimente Exchange precum: direcția traficului e-mail, evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate), măsurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau plasarea în carantină a fișierului, ștergerea sau respingerea e-mail-ului)

Carantină:

1. Produsul trebuie să permită restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă.
2. Locația, fișierele și administrarea Carantinei trebuie să fie efectuată central din consola de management.

Utilizatori:

1. Administrarea este necesar să fie efectuată pe bază de roluri multiple predefinite : Administrator companie, Administrator rețea, Reporter și alte roluri configurabile detaliat cu posibilitatea de selectare a serviciilor și obiectelor pentru care un utilizator poate face modificări.
2. Utilizatorii să poată fi importați din Microsoft Active Directory sau creați în consola de management.
3. Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp.

Log-uri:

1. Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare.

Actualizari:

Soluția trebuie să:

1. Permită definirea de locații de actualizare multiple.
2. Permită activarea/dezactivarea actualizărilor de produs și semnături.
3. Ofere posibilitatea ca orice client antivirus să poată fi configurat să ofere update-urile către alt client antivirus;
4. Permită testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare va include 2 tipuri de actualizări de produs:
 5. Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei;
 6. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc);
7. Permită stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management.

Protecție stații și servere fizice și virtualizate – caracteristici minime:

Soluția antivirus trebuie să:

1. Permită instalarea personalizată a modulelor,
2. includă un vaccin anti-ransomware, cu actualizări de la producător, pentru protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și blocarea procesului de criptare.
3. Includă protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate).
4. Includă module avansate de securitate, proiectate special pentru a detecta atacuri avansate și activități suspecte în faza pre-execuție, pentru protecție împotriva: atacurilor direcționate (Targeted Attack - APT), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware cu posibilitatea de stabilire a nivelului de protecție dorit: permisiv, normal, agresiv cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare.
5. Includă un sandbox în cloud-ul producătorului, ce va putea trimite manual sau automat fișiere, unde vor putea fi „detonate” pentru o analiză în profunzime.

6. Include două variante de analiza a sandbox-ului: doar monitorizare sau blocare cu două tipuri de acțiuni de remediere: implicită și de siguranță. Pentru acțiunea implicită: doar raportare, dezinfectie, ștergere și transmitere în carantină. Pentru acțiunea de siguranță: ștergere sau permutare în carantină;

7. Modulul de Sandbox va include și posibilitatea de trimitere manuala a fișierelor în Sandbox-ul din cloud-ul producătorului. Astfel, dacă administratorul suspectează un fișier ca fiind malițios, îl poate trimite manual în Sandbox pentru a fi „detonat” și a afla verdictul. Va putea trimite mai multe fișiere de odată, cu posibilitate de a specifica dacă vor fi „detonate” individual sau toate în același timp. Acest modul va putea suporta „detonarea” următoarelor tipuri de fișiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML. Aceste fișiere menționate anterior, vor putea fi detectate corect chiar dacă sunt incluse în arhive de tipul: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

Administrare și instalare remote:

1. Pachetele de instalare trebuie să fie configurabile cu modulele necesare: firewall, content control, device control, power user.
2. Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management. Instalarea se va putea face în mai multe moduri:
 - prin descărcarea directă a pachetului pe stația pe care se va face instalarea;
 - prin instalarea la distanță, direct din consola de management
 - remiterea pe email (oricâte adrese) a pachetului de instalare pentru Windows, Linux, Mac.
3. Consola trebuie să includă o secțiune, „Audit”, unde se vor păstra toate acțiunile întreprinse de administratori și utilizatori ai consolei, cu informații detaliate: logare, editare, creare, delogare, permutare etc.
4. Produsul trebuie să ofere posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
5. Produsul trebuie să permită selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domen.
6. Produsul va oferi posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), servere (fizice și/sau virtuale), exchange;

Caracteristici și funcționalități principale ale modulului antivirus

Produsul trebuie să permită:

1. Stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni:
2. Implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune.
3. Alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină.
4. Acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune.
5. Acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină.

6. Scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese, să nu scaneze arhive sau fișiere mai mari de « x » MB, definirea nivelelor de profunzime pentru scanarea în arhive.
7. Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de viruși necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă.
8. Scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc).
9. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP.
10. Definirea până la 16 nivele de profunzime pentru scanarea în arhive.
11. Configurarea căilor ce urmează a fi scanate la cerere.
12. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware.
13. Setarea priorităților scanărilor programate.
14. Configurarea scanării în cloud sau pe mașina de scanare instalată în rețea și parțial scanarea locală pentru stațiile ce nu au suficiente resurse hardware
15. Administratorului să personalizeze și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare: scanare locală, scanarea hibrid cu motoare light, scanarea centralizată în Cloud-ul privat, scanare centralizată cu fallback* pe scanare locală, scanare centralizată cu fallback* pe scanare hibrid.
16. Setarea a tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazate pe monitorizarea proceselor.
17. Scanarea paginilor web.
18. Setarea a unei parole pentru protecția la dezinstalare.
19. Modul de antiphishing.
20. Protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată.
21. Instalarea clientului pe mașinile virtuale parte a unui pool doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale.

Firewall:

1. Să ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
2. Modulul să poată fi instalat/dezinstalat la cerere.
3. Să permită definirea de rețele de încredere pentru mașina destinație.

Protectia datelor:

1. Produsul trebuie să permită blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.

Controlul conținutului:

Produsul trebuie să ofere un modul integrat dedicat controlului accesului la Internet cu următoarele particularități: blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini, blocarea accesului la Internet pe intervale orare, blocarea paginilor de internet care conțin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, blocarea accesului la anumite aplicații definite de administrator, restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violență, pornografie etc).

Controlul aplicațiilor:

Produsul trebuie să aibă un modul pentru administrarea și inventarierea eficientă produselor care să dețină un modul care va oferi posibilitatea de a:

1. Efectua descoperirea aplicațiilor utilizate pe stațiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe.
2. Regăsi toate procesele descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe.
3. Bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subproces) după: cale fișier: local, CD-ROM, portabil sau rețea, hash, certificat.

Controlul dispozitivelor:

Produsul trebuie să conțină un modul pentru controlul dispozitivelor care:

4. Poate fi instalat/dezinstalat conform setărilor stabilite.
5. Permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security Policies 153, IEEE 1284.4, IEEE 1394, Imaging Devices, Modems, Tape Drives, Windows Portable, COM/LPT Ports, SCSI Raid, Printers, Network Adapters, Wireless Network Adapters, Internal and External Storage.
6. Permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client.
7. Permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

Power User:

Produsul trebuie să conțină un modul pentru setări specifice – power user care să:

1. Poată fi instalat/dezinstalat în funcție de preferința administratorului.
2. Permită posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa și modifica setările clientului antivirus dintr-o consola disponibilă local pe mașina client.
3. Permită administratorului soluției să suprascrie din consola setările aplicate de utilizatorii Power User.

Actualizare:

Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor:

1. La nivel de stație în mod silențios (fără avertizări).
2. Folosind unul sau mai multe servere de actualizare.
3. Pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare.

Protecție și securitate pentru telefoane mobile de tip smartphone:

Produsul trebuie să ofere client de protecție pentru dispozitive mobile cu platforma Android (de la v. 2.2) și iOS (de la v 5.)

Clientul mobil trebuie să:

1. Permită asocierea unui dispozitiv cu un utilizator din Active Directory.
2. Ofere posibilitatea instalării prin trimiterea unui email către utilizator cu detaliile de instalare.
3. Permită activarea dispozitivului mobil în consola de management prin scanarea unui cod QR.
4. Asigure disponibilitatea pachetele de instalare pe Apple App Store și Google Play.

5. Să poată întreprinde următoarele acțiuni: blocarea dispozitivului; deblocarea dispozitivului; ștergerea datelor și revenirea la setările din fabrica; localizarea dispozitivului; scanarea dispozitivului (doar pentru cele cu sistem de operare Android); criptarea memoriei dispozitivului (doar pentru cele cu sistem de operare Android).
6. Consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel încât utilizatorul să aibă acces total asupra lui (rooted or jailbroken devices).
7. Întreprindă automat acțiuni în cazul în care un dispozitiv nu este conform cu setările dorite: Ignorare; Blocarea accesului; Blocarea dispozitivului; Ștergerea datelor și revenirea la setările din fabrica; Ștergerea dispozitivului din consola.
8. Ofere posibilitatea de a impune blocarea dispozitivelor cu ajutorul unei parole cu complexitate și perioada de expirare configurabilă, posibilitate de autoblocare a dispozitivului după un număr de minute definite de administrator.
9. Ofere posibilitate de a genera mai multe profiluri care vor stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS) dar și unele legate de accesul la anumite pagini de internet. precum: permiterea, blocarea sau programarea pentru anumite zile și intervale orare a accesului la anumite pagini de internet; crearea unor excepții pentru blocarea sau permiterea accesului către anumite pagini de internet.
10. Include posibilitatea de configurare profilurile acces pagini de internet pentru sistemul de operare iOS cu opțiuni de activare sau dezactivare a: utilizării browser-ului Safari; opțiunii de completare automată a informațiilor; alertării utilizatorului în cazul accesării unor pagini frauduloase; Javascript; Pop-up-urilor; Cookie-uri.

Protecție și securitate pentru serverele de mail Microsoft Exchange

Soluția de protecție a serverelor de Exchange trebuie să:

1. Ofere protecție antivirus, antispam (inclusiv antiphishing), precum și filtrare de atașamente și conținut, prin integrarea cu serverul Microsoft Exchange cu posibilitatea de scanarea antivirus la cerere a bazelor de date Exchange.
2. Asigure scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail.
3. Asigure actualizarea antivirus automat la un interval de maxim 1 ora, precum și la cerere.
4. Include, pe lângă detecția pe baza de semnături, scanarea euristică comportamentală pentru a proteja sistemul de viruși necunoscuți prin detectarea codurilor.
5. Ofere opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfecare, ștergere, mutare în carantină).
6. Ofere protecție anti-spyware (cu bază de semnături actualizabilă) pentru a preveni furtul de date confidențiale.
7. Ofere protecție antispam (cu o bază de semnături actualizabilă. Modulul antispam va trebui să includă un filtru URL cu o bază de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automată a mesajelor scrise cu caractere chirilice sau asiatice.
8. Ofere filtru RBL care să identifice spam-ul prin sincronizarea cu anumite baze de date online care conțin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje.
9. Ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute.
10. Ofere posibilitatea de a defini politici de filtrare antivirus, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori.

11. Asigure actualizarea produsului va fi configurabilă și se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu.
12. Ofere statistici atât referitoare la scanarea antivirus cât și la scanarea antispam.
13. Să integreze în cadrul consolei de management unitar al soluției antivirus în consola centrală unică.

Alte cerințe:

Perioada de suport local și mentinere de la producător:

1. Pentru soluția oferită se solicită a fi 12 luni pentru perioada de suport local și mentinere de la producător;
2. Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță, inclusiv suport local în limba română sau rusă din partea partenerului;
3. Ofertantul va prezenta autorizarea de la producător pentru produsul și suportul livrat;
4. Ofertantul trebuie să aibă minim 2 persoane tehnice calificate pe produsul oferit;
5. Se va oferi manual de instalare și administrare a produsului oferit în limba română și engleză.
6. Compania învingătoare trebuie să prezinte până la semnarea contractului pachetul antivirus (consolă de management, etc) pentru a verifica în practică dacă produsul dat corespunde cerințelor cerute;
7. Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă;
8. Termen de livrare: maxim 10 zile de la data semnării contractului.

3. Pregătirea ofertelor

3.1.	Oferte alternative:	<i>nu vor fi acceptate</i>
3.2.	Garanția pentru ofertă:	<p><i>Oferta va fi însoțită de o Garanție pentru ofertă (emisă de o bancă comercială) conform formularului F3.2 din secțiunea a 3-a – Formulare pentru depunerea ofertei;</i></p> <p><i>Sau, prin transfer la contul autorității contractante, conform următoarelor date bancare:</i></p> <p>Beneficiarul plății: Instituția Publică "Centrul de Tehnologii Informaționale în Finanțe"</p> <ul style="list-style-type: none"> - Cod IBAN: MD86TRPCCC518430A01338AA - Codul băncii: TREZMD2X - Banca: Ministerul Finanțelor – Trezoreria de Stat - Cod fiscal: 1005600036924 - Cod TVA 7800104 <p><i>cu nota "Pentru garanția pentru ofertă la procedura de achiziție publică nr. MTender ID ocds-b3wdp1-MD-1616657521500"</i></p>
3.3.	Garanția pentru ofertă va fi în valoare de:	<i>1% din valoarea ofertei fără TVA.</i>
3.4.	Ediția aplicabilă a Incoterms și termenii comerciali acceptați vor fi (după caz):	<i>INCOTERMS 2010 DDP</i>

3.5.	Termenul de livrare:	<i>licențele vor fi prelungite din data de 10.05.2020, pe un termen de 12 luni</i>
3.6.	Locul livrării bunurilor:	<i>mun. Chișinău, str. C. Tănase 7</i>
3.7.	Metoda și condițiile de plată vor fi:	Achitarea va fi efectuată utilizând sistemul „e-factura” în termen de 15 (cincisprezece) zile bancare din data facturării.
3.8.	Perioada valabilității ofertei va fi de:	<i>45 zile</i>
3.9.	Ofertele în valută străină:	<i>nu se acceptă</i>

4. Depunerea și deschiderea ofertelor

4.1	Locul/Modalitatea de depunere a ofertelor , este:	<i>SIA „RSAP”</i>
4.2.	Termenul limită de depunere a ofertelor este:	<i>conform datelor SIA „RSAP”</i>
4.3.	Persoanele autorizate să asiste la deschiderea ofertelor (cu excepția cazului când ofertele au fost depuse prin SIA “RSAP”).	<i>Ofertanții sau reprezentanții acestora au dreptul să participe la deschiderea ofertelor, cu excepția cazului când ofertele au fost depuse prin SIA „RSAP”</i>

5. Evaluarea și compararea ofertelor

5.1.	Prețurile ofertelor depuse în diferite valute vor fi convertite în:	<i>Ofertele în valută străină: nu se acceptă.</i>
	Sursa ratei de schimb în scopul convertirii:	-
	Data pentru rata de schimb aplicabilă va fi:	-
5.2.	Modalitatea de efectuare a evaluării:	<i>Evaluarea va fi efectuată: pe lot.</i>
5.3.	Factorii de evaluare vor fi următorii:	<i>corespunderea cerințelor tehnice la prețul cel mai scăzut.</i>

6. Adjudecarea contractului

6.1.	Criteriul de evaluare aplicat pentru adjudecarea contractului va fi:	<i>După criteriul: prețul cel mai scăzut.</i>
6.2.	Suma Garanției de bună execuție (se stabilește procentual din prețul contractului adjudecat):	3 %
6.3.	Garanția de bună execuție a contractului:	<p><i>Garanția de buna execuție (emisă de o bancă comercială) conform formularului F3.4</i></p> <p><i>Sau,</i></p> <p><i>prin transfer la contul autorității contractante, conform următoarelor date bancare:</i></p> <p><i>Beneficiarul plății: Instituția Publică ”Centrul de Tehnologii Informaționale în Finanțe”</i></p> <ul style="list-style-type: none"> - <i>Cod IBAN: MD86TRPCCC518430A01338AA</i> - <i>Codul băncii: TREZMD2X</i> - <i>Banca: Ministerul Finanțelor – Trezoreria de Stat</i> - <i>Cod fiscal: 1005600036924</i> - <i>Cod TVA 7800104</i> <p><i>cu nota “Pentru garanția pentru ofertă la procedura de achiziție publică nr. MTender ID ocds-b3wdp1-MD-1616657521500</i></p>
6.4.	Forma de organizare juridică pe care trebuie să o ia asocierea grupului de operatori economici cărora li s-a atribuit contractul	<p>a) Societate pe acțiuni</p> <p>b) Societate cu răspundere limitată</p> <p>c) Altele _____</p>
6.5.	Numărul maxim de zile pentru semnarea și prezentarea contractului către autoritatea contractantă, de la remiterea acestuia spre semnare:	<i>15 zile</i>

Conținutul prezentei Fișe de date a achiziției este identic cu datele procedurii din cadrul Sistemului Informațional Automatizat “REGISTRUL DE STAT AL ACHIZIȚIILOR PUBLICE”. Grupul de lucru pentru achiziții confirmă corectitudinea conținutului Fișei de date a achiziției, fapt pentru care poartă răspundere conform prevederilor legale în vigoare.

Conducătorul grupului de lucru pentru achiziții: _____ Vadim MUNTEAN

CAPITOLUL III
FORMULARE PENTRU DEPUNEREA OFERTEI

Următoarele tabele și formulare vor fi completate de către ofertant și incluse în ofertă.

Formular	Denumirea
F3.1	Formularul ofertei
F3.2	Garanția pentru ofertă – formularul garanției bancare
F3.3	Garanție de bună execuție

Formularul ofertei (F3.1)

[Ofertantul va completa acest formular în conformitate cu instrucțiunile de mai jos. Nu se vor permite modificări în formatul formularului, precum și nu se vor accepta înlocuiri în textul acestuia.]

Data depunerii ofertei: „___” _____ 20__

Procedura de achiziție Nr.: _____

Anunț de participare Nr.: _____

Către: _____

[numele deplin al autorității contractante]

declară că:

[denumirea ofertantului]

a) Au fost examinate și nu există rezervări față de documentele de atribuire, inclusiv modificările nr. _____.

[introduceți numărul și data fiecărei modificări, dacă au avut loc]

b) _____ se angajează să

[denumirea ofertantului]

presteze, în conformitate cu documentele de atribuire și condițiile stipulate în specificațiile tehnice și preț, următoarele servicii _____.

[introduceți o descriere succintă a serviciilor]

c) Suma totală a ofertei fără TVA constituie:

[introduceți prețul pe loturi (unde e cazul) și totalul ofertei în cuvinte și cifre, indicând toate sumele și valutele respective]

d) Suma totală a ofertei cu TVA constituie:

[introduceți prețul pe loturi (unde e cazul) și totalul ofertei în cuvinte și cifre, indicând toate sumele și valutele respective]

e) Prezenta ofertă va rămâne valabilă pentru perioada de timp specificată în **FDA3.8.**, începând cu data-limită pentru depunerea ofertei, în conformitate cu **FDA4.2.**, va rămâne obligatorie și va putea fi acceptată în orice moment pînă la expirarea acestei perioade;

f) În cazul acceptării prezentei oferte, _____

[denumirea ofertantului]

se angajează să obțină o Garanție de bună execuție în conformitate cu **FDA6**, pentru executarea corespunzătoare a contractului de achiziție publică.

g) Nu sîntem în nici un conflict de interese, în conformitate cu art. 74 din Legea nr. 131 din 03.07.2015 privind achizițiile publice.

h) Compania semnatară, afiliații sau sucursalele sale, inclusiv fiecare partener sau subcontractor ce fac parte din contract, nu au fost declarate neeligibile în baza prevederilor legislației în vigoare sau a regulamentelor cu incidență în domeniul achizițiilor publice.

Semnat: _____

[semnătura persoanei autorizate pentru semnarea ofertei]

Nume: _____

În calitate de: _____

[funcția oficială a persoanei ce semnează formularul ofertei]

Ofertantul: _____

Adresa: _____

Data: “___” _____ 20__

Garanția pentru oferta (Garanția bancară) (F3.2)

[Banca emitentă va completa acest formular de garanție bancară în conformitate cu instrucțiunile indicate mai jos. Garanția bancară se va imprima pe foaie cu antetul băncii, pe hârtie specială protejată.]

_____ [Numele băncii și adresa oficiului sau a filialei emitente]
Beneficiar: _____
_____ [numele și adresa autorității contractante]

Data: “ ___ ” _____ 20__

GARANȚIE DE OFERTĂ Nr. _____

_____ a fost informată că
_____ [denumirea băncii]

_____ (numit în continuare „Ofertant”)
_____ [numele ofertantului]

urmează să înainteze oferta către Dvs. la data de “ ___ ” _____ 20__ (numită în
continuare „ofertă”) pentru livrarea/prestarea _____

_____ [obiectul achiziției]
conform anunțului de participare nr. _____ din “ ___ ” _____
20__.

La cererea Ofertantului, noi, _____, prin prezenta,
_____ [denumirea băncii]

ne angajăm în mod irevocabil să vă plătim orice sumă sau sume ce nu depășesc în total suma de:

_____ ([suma în cifre] _____ ([suma în cuvinte])

la primirea de către noi a primei solicitări din partea Dvs. în scris, însoțite de o declarație în care se specifică faptul că Ofertantul încalcă una sau mai multe dintre obligațiile sale referitor la condițiile ofertei, și anume:

- a) și-a retras oferta în timpul perioadei valabilității ofertei sau a modificat oferta după expirarea termenului-limită de depunere a ofertelor; sau
- b) fiind anunțat de către autoritatea contractantă, în perioada de valabilitate a ofertei, despre adjudecarea contractului: (i) eșuează sau refuză să semneze formularul contractului; sau (ii) eșuează sau refuză să prezinte garanția de bună execuție, dacă se cere conform condițiilor procedurii de achiziție, ori nu a executat vreo condiție specificată în documentele de atribuire, înainte de semnarea contractului de achiziție.

Această garanție va expira în cazul în care ofertantul devine ofertant câștigător, la primirea de către noi a copiei înștiințării privind adjudecarea contractului și în urma emiterii Garanției de bună execuție eliberată către Dvs. la solicitarea Ofertantului.

Prezenta garanție este valabilă pînă la data de “ ___ ” _____ 20__.

_____ [semnătura autorizată a băncii]

Garanție de bună execuție (F3.3)

[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 invitației la procedura de achiziție nr. din _____. 201_ [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 documentelor de atribuire.

În urma solicitării Furnizorul/Prestatorul ui, 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],¹ 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]

¹ Autoritatea contractantă trebuie să țină cont de situațiile cînd, în cazul unei extinderi a perioadei de executare a Contractului, autoritatea contractantă va avea nevoie să ceară o extindere și a acestei garanții de la bancă. O astfel de cerere trebuie să fie întocmită în scris și trebuie făcută înainte de expirarea datei stabilite în garanție. În procesul pregătirii acestei Garanții, autoritatea contractantă ar putea lua în considerare adăugarea următorului text în formular, la sfîrșitul penultimului paragraf: „Noi sîntem de acord cu o singură extindere a acestei Garanții pentru o perioadă ce nu depășește [șase luni] [un an], ca răspuns al cererii în scris a autorității contractante pentru o astfel de extindere, și o astfel de cerere urmează a fi prezentată nouă înainte de expirarea prezentei garanții.”

CAPITOLUL IV
SPECIFICAȚII TEHNICE ȘI DE PREȚ

Următoarele tabele și formulare vor fi completate de către ofertant și incluse în ofertă. În cazul unei discrepanțe sau al unui conflict cu textul CAPITOLULUI I, prevederile din prezentul CAPITOL vor prevala asupra prevederilor din CAPITOLUL I.

Formular	Denumirea
F4.1	Specificații tehnice
F4.2	Specificații de preț

Specificații tehnice (F4.1)

[Acest tabel va fi completat de către ofertant în coloanele 3, 4, 5, 7, iar de către autoritatea contractantă – în coloanele 1, 2, 6, 8]

Numărul procedurii de achiziție: MTender ID ocds-b3wdp1-MD-1616657521500

Denumirea procedurii de achiziție: Pachet software antivirus (prelungirea licențelor)

Cod CPV	Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificare a tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7	8
48761000-0	Pachet software antivirus				<p>Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST) și să fie prezent în mențiunile Gartner. Satisfacerea necesităților minime va constitui 500 licențe (workstation PC, mailboxes), și 100 licențe (VDI/VS/Server), în scopul managementului centralizat pentru dispozitive.</p> <p>Licențele oferite trebuie să fie capabile să prelungească pe un termen de 12 luni, licențele existente compatibile sau echivalente pentru Bitdefender Gravity Zone Elite.</p> <p>Caracteristici generale ale produsului: Produsul va conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management:</p> <ol style="list-style-type: none"> Protecție stații și servere fizice și virtualizate: <ul style="list-style-type: none"> Windows 10,8.1,7, Vista (SP1), XP (SP3), Mac OS X 10.12.x, 10.11.x, 10.10.x, 10.9.x, 10.8.x Windows Server 2003/2008/2008/2019 R2/2012/2012 R2/2016. Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Oracle Linux 6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual, Debian 5.0 sau mai recent. Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS și Android. 		

				<p>3. Protecție și securitate de tip „sandboxing” pentru serverele și stațiile de lucru;</p> <p>4. Controlul dispozitivelor, controlul accesului la Internet, filtrarea traficului prin modul de tip firewall pentru mașinile fizice și virtuale</p> <p>5. Protecție și securitate pentru serverele email Microsoft Exchange.</p> <p>Consola de management: Pachetul de instalare va fi oferit ca un appliance virtual. Aceasta din urmă nu va necesita o licență suplimentară pentru sistemul de operare, iar imaginea de tip template va fi posibil de a fi importată în următoarele platforme de virtualizare: VMware vSphere, Citrix XenServe, Microsoft Hyper-V, Red Hat Enterprise Virtualization, KVM, Oracle VM.</p> <p>Consola de management va fi oferită cu o bază de date inclusă, non-relațională. Soluția trebuie să:</p> <ol style="list-style-type: none"> 1. Fie scalabilă, astfel ca oricare dintre roluri sau servicii să poată fi instalate separat sau împreună pe aceeași sau mai multe VDI-uri. 2. Asigure următoarele roluri: server cu baza de date, server de comunicație, server de actualizare, server de web. 3. Asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale VMware și Citrix prin task din consola de management. 4. Includă un modul load balancer pentru performanța și redundanță 5. Includă mecanisme de configurare a disponibilității pentru serverul cu baze de date (clustering). 6. Includă posibilitatea de a fi accesată atât de pe stațiile de lucru cât și de pe dispozitivele mobile (tabletă, smartphone). <p>Interfața consolei de management va fi în limba română. Interfața agentului care se instalează pe stații de lucru și servere, va fi în limba română.</p> <p>Cerințe generale produs: Soluția trebuie să:</p> <ol style="list-style-type: none"> 1. Includă unul sau mai multe module de update server prin care să asigure actualizarea componentelor și a semnăturilor. 2. Permită activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management. 3. Transmită alerte de ne funcționalitate, cu 30 de minute înainte de actualizare. 4. Permită vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi și îmbunătățiri, probleme rezolvate, probleme cunoscute 5. Afișeze notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție viruși, actualizări de produs disponibile). 6. Permită integrarea cu un server Syslog pentru raportarea evenimentelor antivirus. 7. Permită instalarea serviciului de SMNP pentru raportarea statusului mașinilor din cadrul componentei de management. 		
--	--	--	--	--	--	--

				<p>8. Permite crearea unei copii de siguranta a bazei de date a consolei de administrare, la cerere sau programat, stocata local, pe un server FTP sau in retea</p> <p>Inventarierea retelei – managementul securitatii</p> <p>Produsul trebuie sa:</p> <ol style="list-style-type: none"> 1. Se integreze cu domenii Active Directory multiple, VMware vCenter, Citrix Xen si sa importe inventarul acestor platforme. 2. Permite descoperirea masinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM. 3. Permite descoperirea statiilor fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery. 4. ofere optiuni de cautare, sortare si filtrare dupa numele sistemului, sistem de operare si adresa IP. 5. Permite instalarea la distanta sau manual a clientilor antivirus pe masini fizice si virtuale. 6. Permite selectarea modulelor componente atunci cand se creeaza pachetul clientului care se Instaleaza pe masinile fizice/virtuale. 7. Permite lansarea de task-uri de scanare, actualizare, instalare, deinstalare la distanta pentru clientul antivirus. 8. Ofere posibilitatea de repornire a masinilor fizice de la distanta. 9. Ofere informatii detaliate despre fiecare task inițiat si afisarea statutului lui. 10. Permite configurarea centralizata a clientilor antivirus prin intermediul politicilor. 11. Ofere in consola de management informatii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnatura. 12. Permite descoperirea tuturor aplicatiilor instalate pe toate statiile si serverele din retea. 13. Permite crearea unui pachet unic pentru toate sistemele de operare, de statii sau servere. Astfel, administratorul va putea descarca pachetele pentru protectia statiilor si serverelor pe care ruleaza sistemul de operare Windows, Linux si Mac. <p>Politici:</p> <p>Produsul trebuie sa:</p> <ol style="list-style-type: none"> 1. Permite configurarea setarilor clientului antivirus prin intermediul unei singure politici ce contine setari pentru toate module 2. Contina optiuni specifice de activare/dezactivare si configurare a functionalitatilor precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicatiilor, scanarea traficului web, controlul dispozitivelor, power user. 3. Permite aplicarea politicilor pe masini client, grupuri de masini, pool-uri de resurse (VMware), domeniu, unitati organizationale sau useri de active directoy. 4. Poata fi schimbata automat in functie de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este in accesai retea cu infrastructura de management, Tipul retelei (lan, wireless). <p>Monitorizare si raportare:</p>		
--	--	--	--	---	--	--

				<p>Produsul trebuie să:</p> <ol style="list-style-type: none">1. Permită setarea de opțiuni specifice pentru afișarea rapoartelor existente.2. Dețină un panou central care să afișeze statutul modulelor și rapoartele lor pentru perioadele de timp specificate.3. Conțină rapoarte care prezintă statusul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.4. Trimită rapoarte către un număr nelimitat de adrese de email.5. Permită vizualizarea rapoartelor curente programate de administrator.6. Permită exportarea rapoartelor în format .pdf și detaliile ca format .csv.7. Includă un generator de rapoarte care să ofere posibilitatea de a investiga o problemă de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal, evenimente Exchange.8. Ofere interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor.9. Ofere interogări legate de evenimente precum: calculatorul ținta pe care a avut loc evenimentul, tipul starea și configurația agentului de securitate instalat, starea modulelor și rolurilor de protecție instalate pe agentul de securitate, denumirea și alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicații blocate, detecțiile etc)10. Ofere interogări de evenimente Exchange precum: direcția traficului e-mail, evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate), măsurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau plasarea în carantină a fișierului, ștergerea sau respingerea e-mail-ului) <p>Carantină:</p> <ol style="list-style-type: none">1. Produsul trebuie să permită restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă.2. Locația, fișierele și administrarea Carantinei trebuie să fie efectuată central din consola de management. <p>Utilizatori:</p> <ol style="list-style-type: none">1. Administrarea este necesar să fie efectuată pe bază de roluri multiple predefinite : Administrator companie, Administrator rețea, Reporter și alte roluri configurabile detaliat cu posibilitatea de selectare a serviciilor și obiectelor pentru care un utilizator poate face modificări.2. Utilizatorii să poată fi importați din Microsoft Active Directory sau creați în consola de management.3. Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp. <p>Log-uri:</p> <ol style="list-style-type: none">1. Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare.		
--	--	--	--	--	--	--

				<p>Actualizari:</p> <p>Soluția trebuie să:</p> <ol style="list-style-type: none"> 1. Permită definirea de locații de actualizare multiple. 2. Permită activarea/dezactivarea actualizărilor de produs si semnături. 3. Ofere posibilitatea ca orice client antivirus să poată fi configurat să ofere update-urile către alt client antivirus; 4. Permită testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile si serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare va include 2 tipuri de actualizări de produs: 5. Ciclu rapid, gândit pentru un mediu de test in cadrul rețelei; 6. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc); 7. Permită stabilirea zonelor de test si critice din cadrul rețelei prin intermediul politicilor din consola de management. <p>Protecție stații și servere fizice si virtualizate – caracteristici minime:</p> <p>Soluția antivirus trebuie să:</p> <ol style="list-style-type: none"> 1. Permită instalarea personalizată a modulelor, 2. includă un vaccin anti-ransomware, cu actualizări de la producător, pentru protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar daca sunt infectate și blocarea procesului de criptare. 3. Includă protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate). 4. Includă module avansate de securitate, proiectate special pentru a detecta atacuri avansate și activități suspecte în faza pre-execuție, pentru protecție împotriva: atacurilor direcționate (Targeted Attack - APT), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware cu posibilitatea de stabilire a nivelului de protecție dorit: permisiv, normal, agresiv cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare. 5. Includă un sandbox în cloud-ul producătorului, ce va putea trimite manual sau automat fișiere, unde vor putea fi „detonate” pentru o analiză în profunzime. 6. Includă două variante de analiza a sandbox-ului: doar monitorizare sau blocare cu două tipuri de acțiuni de remediere: implicită și de siguranța. Pentru acțiunea implicită: doar raportare, dezinfectie, ștergere și transmitere în carantină. Pentru acțiunea de siguranța: ștergere sau permutare în carantină; 7. Modulul de Sandbox va include si posibilitatea de trimitere manuala a fișierelor in Sandbox-ul din cloud-ul producătorului. Astfel, daca administratorul suspectează un fișier ca fiind malițios, îl poate trimite manual in Sandbox pentru a fi „detonat” si a afla verdictul. Va putea trimite mai multe fișiere de odată, cu posibilitate de a specifica daca vor fi „detonate” individual sau toate in același timp. Acest modul va poate suporta „detonarea” următoarelor tipuri de fișiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML. Aceste fișiere menționate anterior, vor putea fi detectate corect chiar daca sunt incluse in arhive de tipul: 		
--	--	--	--	--	--	--

				<p>7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.</p> <p>Administrare și instalare remote:</p> <ol style="list-style-type: none"> 1. Pachetele de instalare trebuie să fie configurabile cu modulele necesare: firewall, content control, device control, power user. 2. Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management. Instalarea se va putea face în mai multe moduri: <ul style="list-style-type: none"> - prin descărcarea directă a pachetului pe stația pe care se va face instalarea; - prin instalarea la distanță, direct din consola de management - remiterea pe email (oricâte adrese) a pachetului de instalare pentru Windows, Linux, Mac. 3. Consola trebuie să includă o secțiune, „Audit”, unde se vor păstra toate acțiunile întreprinse de administratori și utilizatori ai consolei, cu informații detaliate: logare, editare, creare, delogare, permutare etc. 4. Produsul trebuie să ofere posibilitatea de a crea pachetele de instalare de tip web installer sau kit full. 5. Produsul trebuie să permită selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domen. 6. Produsul va oferi posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), servere (fizice și/sau virtuale), exchange; <p>Caracteristici și funcționalități principale ale modulului antivirus</p> <p>Produsul trebuie să permită:</p> <ol style="list-style-type: none"> 1. Stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni: 2. Implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune. 3. Alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină. 4. Acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune. 5. Acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină. 6. Scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese, să nu scaneze arhive sau fișiere mai mari de « x » MB, definirea nivelelor de profunzime pentru scanarea în arhive. 7. Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de viruși necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă. 8. Scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). 9. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP. 10. Definirea până la 16 nivele de profunzime pentru scanarea în arhive. 	
--	--	--	--	--	--

				<p>11. Configurarea căilor ce urmează a fi scanate la cerere.</p> <p>12. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware.</p> <p>13. Setarea priorităților scanărilor programate.</p> <p>14. Configurarea scanării în cloud sau pe mașina de scanare instalată în rețea și parțial scanarea locală pentru stațiile ce nu au suficiente resurse hardware</p> <p>15. Administratorului să personalizeze și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare: scanare locală, scanarea hibrid cu motoare light, scanarea centralizată în Cloud-ul privat, scanare centralizată cu fallback* pe scanare locală, scanare centralizată cu fallback* pe scanare hibrid.</p> <p>16. Setarea a tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazate pe monitorizarea proceselor.</p> <p>17. Scanarea paginilor web.</p> <p>18. Setarea a unei parole pentru protecția la dezinstalare.</p> <p>19. Modul de antiphishing.</p> <p>20. Protecție în timp real pe mașinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalată.</p> <p>21. Instalarea clientului pe mașinile virtuale parte a unui pool doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale.</p> <p>Firewall:</p> <ol style="list-style-type: none"> 1. Să ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. 2. Modulul să poată fi instalat/dezinstalat la cerere. 3. Să permită definirea de rețele de încredere pentru mașina destinație. <p>Protecția datelor:</p> <ol style="list-style-type: none"> 1. Produsul trebuie să permită blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. <p>Controlul conținutului:</p> <p>Produsul trebuie să ofere un modul integrat dedicat controlului accesului la Internet cu următoarele particularități: blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini, blocarea accesului la Internet pe intervale orare, blocarea paginilor de internet care conțin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, blocarea accesului la anumite aplicații definite de administrator, restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violența, pornografie etc).</p> <p>Controlul aplicațiilor:</p> <p>Pentru administrare și inventariere eficientă produsul trebuie să dețină un modul care va oferi posibilitatea de a:</p>	
--	--	--	--	---	--

				<p>1. Efectua descoperirea aplicațiilor utilizate pe stațiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe.</p> <p>2. Regăsi toate procesele descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe.</p> <p>3. Bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subprocesse) după: cale fișier: local, CD-ROM, portabil sau rețea, hash , certificat.</p> <p>Controlul dispozitivelor: Produsul trebuie să conțină un modul pentru controlul dispozitivelor care:</p> <p>4. Poate fi instalat/dezinstalat conform setărilor stabilite.</p> <p>5. Permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security Policies 153, IEEE 1284.4, IEEE 1394, Imaging Devices, Modems, Tape Drives, Windows Portable, COM/LPT Ports, SCSI Raid, Printers, Network Adapters, Wireless Network Adapters, Internal and External Storage.</p> <p>6. Permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client.</p> <p>7. Permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.</p> <p>Power User: Produsul trebuie să conțină un modul pentru setări specifice – power user care să:</p> <p>1. Poată fi instalat/dezinstalat în funcție de preferința administratorului.</p> <p>2. Permită posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa și modifica setările clientului antivirus dintr-o consola disponibilă local pe mașina client.</p> <p>3. Permită administratorului soluției să suprascrise din consola setările aplicate de utilizatorii Power User.</p> <p>Actualizare: Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor:</p> <p>1. La nivel de stație în mod silențios (fără avertizări).</p> <p>2. Folosind unul sau mai multe servere de actualizare.</p> <p>3. Pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare.</p> <p>Protecție și securitate pentru telefoane mobile de tip smartphone: Produsul trebuie să ofere client de protecție pentru dispozitive mobile cu platforma Android (de la v. 2.2) și iOS (de la v 5.)</p> <p>Clientul mobil trebuie să:</p> <p>1. Permită asocierea unui dispozitiv cu un utilizator din Active Directory.</p> <p>2. Ofere posibilitatea instalării prin trimiterea unui email către utilizator cu detaliile de instalare.</p> <p>3. Permită activarea dispozitivului mobil în consola de management prin scanarea unui cod QR.</p> <p>4. Asigure disponibilitatea pachetele de instalare pe Apple App Store si Google Play.</p>		
--	--	--	--	---	--	--

				<p>5. Să poată întreprinde următoarele acțiuni: blocarea dispozitivului; deblocarea dispozitivului; ștergerea datelor și revenirea la setările din fabrică; localizarea dispozitivului; scanarea dispozitivului (doar pentru cele cu sistem de operare Android); criptarea memoriei dispozitivului (doar pentru cele cu sistem de operare Android).</p> <p>6. Consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel încât utilizatorul să aibă acces total asupra lui (rooted or jailbroken devices).</p> <p>7. Întreprindă automat acțiuni în cazul în care un dispozitiv nu este conform cu setările dorite: Ignorare; Blocarea accesului; Blocarea dispozitivului; Ștergerea datelor și revenirea la setările din fabrică; Ștergerea dispozitivului din consola.</p> <p>8. Ofere posibilitatea de a impune blocarea dispozitivelor cu ajutorul unei parole cu complexitate și perioada de expirare configurabilă, posibilitate de autoblocare a dispozitivului după un număr de minute definite de administrator.</p> <p>9. Ofere posibilitate de a genera mai multe profiluri care vor stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS) dar și unele legate de accesul la anumite pagini de internet. precum: permiterea, blocarea sau programarea pentru anumite zile și intervale orare a accesului la anumite pagini de internet; crearea unor excepții pentru blocarea sau permiterea accesului către anumite pagini de internet.</p> <p>10. Includă posibilitatea de configurare profilurile acces pagini de internet pentru sistemul de operare iOS cu opțiuni de activare sau dezactivare a: utilizării browser-ului Safari; opțiunii de completare automată a informațiilor; alertării utilizatorului în cazul accesării unor pagini frauduloase; Javascript; Pop-up-urilor; Cookie-uri.</p> <p>Protecție și securitate pentru serverele de mail Microsoft Exchange Soluția de protecție a serverelor de Exchange trebuie să:</p> <ol style="list-style-type: none"> 1. Ofere protecție antivirus, antispam (inclusiv antiphishing), precum și filtrare de atașamente și conținut, prin integrarea cu serverul Microsoft Exchange cu posibilitatea de scanarea antivirus la cerere a bazelor de date Exchange. 2. Asigure scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail. 3. Asigure actualizarea antivirus automat la un interval de maxim 1 ora, precum și la cerere. 4. Includă, pe lângă detecția pe baza de semnături, scanarea euristică comportamentală pentru a proteja sistemul de virușii necunoscuți prin detectarea codurilor. 5. Ofere opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfecare, ștergere, mutare în carantină). 6. Ofere protecție anti-spyware (cu bază de semnături actualizabilă) pentru a preveni furtul de date confidențiale. 7. Ofere protecție antispam (cu o bază de semnături actualizabilă. Modulul antispam va trebui să includă un filtru URL cu o bază de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automată a mesajelor scrise cu caractere chirilice sau asiatice. 		
--	--	--	--	---	--	--

				<p>8. Ofere filtru RBL care să identifice spam-ul prin sincronizarea cu anumite baze de date online care conțin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje.</p> <p>9. Ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute.</p> <p>10. Ofere posibilitatea de a defini politici de filtrare antivirus, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori.</p> <p>11. Asigure actualizarea produsului va fi configurabilă și se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu.</p> <p>12. Ofere statistici atât referitoare la scanarea antivirus cât și la scanarea antispam.</p> <p>13. Să integreze în cadrul consolei de management unitar al soluției antivirus în consola centrală unică.</p> <p>Alte cerințe: Perioada de suport local și menținere de la producător:</p> <ol style="list-style-type: none"> 1. Pentru soluția oferită se solicită a fi 12 luni pentru perioada de suport local și menținere de la producător; 2. Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță, inclusiv suport local în limba română sau rusă din partea partenerului; 3. Ofertantul va prezenta autorizarea de la producător pentru produsul și suportul livrat; 4. Ofertantul trebuie să aibă minim 2 persoane tehnice calificate pe produsul oferit; 5. Se va oferi manual de instalare și administrare a produsului oferit în limba română și engleză. 6. Compania învingătoare trebuie să prezinte până la semnarea contractului pachetul antivirus (consolă de management, etc) pentru a verifica în practică dacă produsul dat corespunde cerințelor cerute; 7. Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă; 8. Termen de livrare: maxim 10 zile de la data semnării contractului. 		
	TOTAL					

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

Ofertantul: _____ Adresa: _____

Specificații de preț (F4.2)

[Acest tabel va fi completat de către ofertant în coloanele 5,6,7,8, iar de către autoritatea contractantă – în coloanele 1,2,3,4,9,10]

Numărul procedurii de achiziție: MTender ID ocds-b3wdp1-MD-1616657521500
--

Denumirea procedurii de achiziție: Pachet software antivirus (prelungirea licențelor)

Cod CPV	Denumirea bunurilor/serviciilor	Unitatea de măsură	Cantitatea	Preț unitar (fără TVA)	Preț unitar (cu TVA)	Suma fără TVA	Suma cu TVA	Termenul de livrare	Clasificație bugetară (IBAN)
1	2	3	4	5	6	7	8	9	10
48761000-0	Pachet software antivirus (prelungirea licențelor)	licențe	600					Din 10.05.2021, pe un termen de 12 luni	

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

Ofertantul: _____ Adresa: _____

CAPITOLUL V
FORMULARUL DE CONTRACT

Formular	Denumirea
F5.1	Contract-model Bunuri



ACHIZIȚII PUBLICE

CONTRACT Nr. _____/COP/2021

**de achiziționare a bunurilor: Pachet software antivirus
(prelungirea licențelor)**

Cod CPV: 48761000-0

/ ____ / ____ / ____

mun. Chișinău

Vînzător	Autoritatea Contractantă
_____ (denumirea completă a întreprinderii, asociației, organizației), IDNO _____, cu sediul _____, reprezentată prin _____, care acționează în baza _____, denumit(a) în continuare Prestator , pe de o parte,	Instituția Publică „Centrul de Tehnologii Informaționale în Finanțe”, IDNO 1005600036924, cu sediul în R. Moldova, mun. Chișinău, str. Constantin Tănase, nr. 7, reprezentată prin Directorul dl Vitalie COCEBAN, care acționează în baza Statutului, denumit(ă) în continuare - „Beneficiar”, pe de altă parte

ambele denumite în continuare *Părți*, au încheiat prezentul Contract referitor la următoarele:

- a. Achiziționarea Pachet software antivirus (prelungirea licențelor), denumite în continuare Bunuri, conform procedurii de achiziții publice de tip cererea ofertelor de prețuri, nr. _____ din _____, în baza deciziei grupului de lucru al Cumpărătorului din „_____” _____ 20 ____.
- b. Următoarele documente vor fi considerate părți componente și integrale ale Contractului:
 - a) Specificația tehnică și de preț
 - b) *Garanție de bună execuție a contractului*
- c. Prezentul Contract va predomina asupra tuturor altor documente componente. În cazul unor discrepante 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 Cumpărător, Vînzătorul se obligă prin prezenta să livreze Cumpărătorului Bunurile și să înlătore defectele lor în conformitate cu prevederile Contractului sub toate aspectele.

Cumpărătorul se obligă prin prezenta să plătească Vînzătorului, în calitate de contravaloare a livrării bunurilor, precum și a înlăturării defectelor lor, prețul Contractului sau orice altă sumă care poate deveni plătită conform prevederilor Contractului în termenele și modalitatea stabilite de Contract.

1. OBIECTUL CONTRACTULUI

1.1. În conformitate cu prezentul Contract, Vânzătorul își asumă obligația de a vinde și livra Pachet software antivirus (prelungirea licențelor) (în continuare – *bunuri*), conform specificației din Anexa nr. 1 la prezentul Contract, care este parte integrantă a acestuia, iar Cumpărătorul se obligă să recepționeze și să achite prețul acestora.

1.2. Cantitatea, sortimentul și specificația este prezentată în Anexa nr.1 la prezentul Contract, care este parte integrantă a acestuia.

2. TERMENI ȘI CONDIȚII DE LIVRARE

2.1. Livrarea bunurilor se va efectua de către Vânzător în condițiile INCOTERMS 2010 DDP la sediul/adresa indicată de către Cumpărător, str. Constantin Tănase, nr. 7, et. II, în termen de 5 (cinci) zile lucrătoare din data primirii solicitării din partea Cumpărătorului, prin comanda telefonică.

3. PREȚUL ȘI CONDIȚIILE DE PLATĂ

3.1. Prețul bunurilor livrate conform prezentului Contract este stabilit în lei moldovenești, fiind indicat în Anexa nr. 1 la prezentul Contract.

3.2. Suma totală a prezentului Contract, constituie: _____ (lei, --bani) lei MDL, inclusiv TVA.

3.3. Achitarea pentru bunurile livrate se va efectua de către Cumpărător prin virament în contul de decontare al Vânzătorului, în termen de 10 (zece) zile calendaristice din data emiterii facturii fiscale, prin intermediul SIA „e-Factura” și a actului de predare-primire a bunurilor.

4. CONDIȚIILE DE PREDARE-PRIMIRE

4.1. Bunurile se consideră livrate de către Vânzător și recepționate de către Cumpărător, dacă cantitatea, sortimentul și specificația bunurilor corespunde informației indicate în documentele de însoțire (actul de predare-primire a bunurilor) precum și integritatea bunurilor corespunde informației indicate în din Anexa nr. 1 la prezentul Contract.

4.2. În cazul în care Cumpărătorul constată că bunurile nu corespund cerințelor tehnice indicate în Specificația din Anexa nr. 1, Părțile vor întocmi un Act de neconformitate, iar Vânzătorul se obligă să remedieze toate defectele constatate la bunurile livrate în condițiile prezentului Contract.

5. STANDARDE

5.1. Bunurile livrate în baza Contractului vor respecta standardele prezentate de către Vânzător, în specificația descrisă în Anexa nr. 1 a prezentului Contract.

5.2. Când nu este menționat nici un standard sau reglementare aplicabilă se vor respecta standardele sau alte reglementări autorizate în țara de origine a bunurilor care urmează a fi livrate și care fac obiectul Contractului dat.

6. OBLIGAȚIILE PĂRȚILOR

6.1. În baza prezentului Contract, Vânzătorul se obligă:

- a) să livreze bunurile în condițiile și termenele prevăzute de prezentul Contract;
- b) să asigure condițiile corespunzătoare pentru recepționarea bunurilor de către Cumpărător, în termenele stabilite, în corespundere cu cerințele prezentului Contract;
- c) 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. JUSTIFICAREA DATORITĂ UNUI IMPEDIMENT

7.1. Părțile sunt exonerate de răspundere pentru neîndeplinirea parțială sau integrală a obligațiilor ce le revin conform prezentului Contract, dacă o astfel de neîndeplinire este cauzată de vreun impediment sau circumstanță care nu depinde de voința Părților (ex: inundația, incendiul, calamități naturale, acțiuni militare, acțiuni ale organelor puterii sau administrației de stat, obligatorii pentru executare, etc.). Lista acestor impedimente nu poate fi exhaustivă.

7.2. Partea care nu-și poate executa obligațiile sale din cauza impedimentului justificator va notifica cealaltă parte despre survenirea acestui impediment și efectele lui asupra capacității de a executa, asupra executării obligațiilor contractuale, neîntârziat, în termen de 3 (trei) zile lucrătoare din momentul apariției lui.

7.3. Partea afectată va lua toate măsurile pentru minimalizarea efectelor impedimentului justificator asupra executării prezentului Contract și va depune cu diligența necesară toate eforturile pentru a le depăși și pentru a-și îndeplini în continuare obligațiile contractuale. Pe toată perioada de existență a impedimentului justificator obligațiile ambelor părți ce decurg din prezentul Contract vor fi prelungite.

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 Vînzătorului de a livra bunurile prevăzute în prezentul Contract;
- b) Cumpărător în caz de nerespectare de către Vînzător a termenelor de livrare a bunurilor;
- c) Vînzător în caz de nerespectare de către Cumpărător a termenelor de plată pentru bunurile livrate;
- d) Vînzător sau Cumpărător în caz de nesatisfacere de către una dintre Părți a pretențiilor înaintate conform prezentului Contract.

8.3. Partea inițiatoare a rezoluțiunii Contractului este obligată să comunice în termen de 5 (cinci) zile lucrătoare celeilalte Părți despre intențiile ei printr-o scrisoare motivată.

8.4. Partea înștiințată este obligată să răspundă în decurs de 5 (cinci) zile lucrătoare de la primirea notificării. În cazul în care litigiul nu este soluționat pe cale amiabilă în termenele stabilite, partea inițiatoare are dreptul să declare Contractul rezolvit, conform situației la data indicată în reclamație.

9. RECLAMAȚII ȘI SANCTIUNI

9.1. Reclamațiile privind cantitatea și sortimentul bunurilor livrate sunt înaintate Vînzătorului la momentul recepționării lor de către Cumpărător, fiind confirmate printr-un act întocmit în comun cu reprezentantul Vînzătorului.

9.2. Pretențiile privind calitatea bunurilor livrate sunt înaintate Vînzătorului în termen de 5 (cinci) zile lucrătoare 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. Vînzătorul este obligat să examineze pretențiile înaintate în termen de 5 (cinci) zile lucrătoare de la data primirii acestora și să comunice Cumpărătorului despre decizia luată.

9.4. În caz de recunoaștere a pretențiilor, Vînzătorul este obligat, în termen de 5 (cinci) zile, să livreze suplimentar Cumpărătorului cantitatea nelivrată de bunuri, iar în caz de constatare a calității necorespunzătoare - să le substituie sau să le remedieze în conformitate cu cerințele Contractului.

9.5. Vînzătorul poartă răspundere pentru calitatea bunurilor livrate în limitele stabilite de legislația în vigoare a Republicii Moldova, 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 partea vinovată.

9.7. Pentru refuzul de a livra Bunurile prevăzut în prezentul Contract, Vînzătorul poartă răspundere (sub formă de penalitate) în mărime de 10% din suma totală a prezentului Contractului.

9.8. Pentru livrarea cu întârziere a Bunurilor, Vînzătorul poartă răspundere materială în valoare de 0,1% din suma Bunurilor nelivrate, pentru fiecare zi de întârziere, dar nu mai mult de 10% din suma totală a prezentului Contract.

9.9. Pentru achitarea cu întârziere, Cumpărătorul poartă răspundere materială în valoare de 0,1% din suma Bunurilor neachitate, pentru fiecare zi de întârziere, dar nu mai mult de 10% din suma totală a prezentului Contract.

10. DISPOZIȚII FINALE

10.1. Litigiile ce 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 în vigoare a Republicii Moldova.

10.2. De la data semnării prezentului Contract, toate negocierile purtate și documentele perfectate anterior își pierd valabilitatea.

10.3. 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.

10.4. Niciuna 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.

10.5. Prezentul Contract este întocmit în 2 (două) exemplare, în limba de stat a Republicii Moldova, câte un exemplar pentru Vînzător și Cumpărător, ambele având aceeași valoare juridică.

10.6. Prezentul Contract reprezintă acordul de voință al ambelor Părți, se consideră încheiat la data semnării lui, fiind valabil până la data de 31.12.2021.

11. Datele juridice, poștale și bancare ale părților

Vînzător	Autoritatea Contractantă
	Instituția Publică „Centrul de Tehnologii Informaționale în Finanțe”
Adresa poștală:	Adresa poștală: mun. Chișinău, str. Constantin Tănase, nr. 7
Telefon:	Telefon: 022-262-872
Cont de decontare:	Cont de decontare: MD86TRPCCC518430A01338AA
Banca:	Banca: Trezoreria de Stat
Cod: MOBBMD22	Cod: TREZMD2X
Cod fiscal: TVA 0607320	Cod fiscal: 1005600036924, TVA 7800104
Director _____	Director Vitalie COCEBAN _____
L.Ș.	L.Ș.

Anexa nr. 1

la Contractul Nr. / _____ /COP/2021

din / ____ / ____ / ____ /

SPECIFICAȚIA BUNURILOR

Nr. d/o	Descrierea bunului	Cantitate	U.M.	Preț unitate inclusiv TVA (lei)	Suma totală inclusiv TVA (lei)
1.	Pachet software antivirus (prelungirea licențelor)	600	licențe	-----	-----
TOTAL, inclusiv TVA:					-----

„Vînzător”	„Cumpărător”
_____	Instituția Publică „Centrul de Tehnologii Informaționale în Finanțe”
Director _____ L.Ș.	Director Vitalie COCEBAN _____ L.Ș.