APROBAT
prin Ordinul
Ministerului Finanțelor
nr. 175 din 05 octombrie 2018

DOCUMENTAŢIA STANDARD

pentru realizarea achiziţiilor publice de bunuri prin cererea ofertelor de prețuri

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

Cod CPV: **48761000-0**

Autoritarea 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
INSTRUCŢIUNI PENTRU OFERTANŢI (IPO)
[Notă: nu se va modifica de către Autoritatea Contractantă]

Secţiunea 1. Dispoziţii generale

1. Scopul procedurii de achiziţie

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 achiziţie

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

a) libera concurenţă;
b) eficienţa utilizării fondurilor publice și minimizarea riscurilor autorităților/entităților contractante;
c) transparenţa;
d) tratamentul egal, imparțial și nedescriminatoriu în privința tuturor ofertanților și operatorilor economici;
e) protecţia mediului;
f) respectarea ordinii de drept;
g) confidenţialitatea;
h) asumarea răspunderii în cadrul procedurilor de achiziţie publică.

3. Sursa de finanţare

3.1. În **FDA** va fi specificată sursa de finanțare pentru plăţile 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 mijoacelor financiare, **FDA** va conține argumentarea justificativă a autorității contractante privind alocarea ulterioară pentru procedura de achiziție curentă.

4. Participanţii la procedura de achiziţie

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 condiţiile Legii nr. 131/2015 privind achiziţiile publice (în continuare Legea nr. 131/2015), la procedura de atribuire a contractului de achiziţii publice.

4.2. Dreptul de participare la procedurile de atribuire a contractelor de achiziţii publice poate fi rezervat de către Guvern unor ateliere protejate şi întreprinderi sociale de inserţie în cazul în care majoritatea angajaţilor implicaţi sînt persoane cu dizabilităţi care, prin natura sau gravitatea deficienţelor lor, nu pot desfăşura o activitate profesională în condiţii normale.

5. Cheltuielile de participare la procedura de achiziţie

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

5.2. La depunerea ofertelor, operatorul economic, după caz, va achita o taxă. Modul de achitare a taxei menţionate, precum şi 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 şi toată corespondenţa dintre ofertant şi autoritatea contractantă vor fi întocmite în limba de stat. Documentele justificative şi literatura de specialitate tipărită, care fac parte din ofertă, pot fi în altă limbă, cu condiţia ca acestea să fie însoţite de o traducere exactă a fragmentelor relevante în limba de stat.

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

7. Secţiunile Documentelor de atribuire

7.1. Documentele de atribuire includ toate secţiunile indicate în prezentul punct şi trebuie citite în conjuncţie cu orice modificare conform punctului IPO8.

CAPITOLUL I. Instrucţiuni pentru ofertanţi
CAPITOLUL II. Fişa de date a achiziţiei
CAPITOLUL III. Formulare pentru depunerea ofertei
CAPITOLUL IV. Specificații tehnice și de preț.
CAPITOLUL V. Formularul de contract

8. Clarificarea şi 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 documentaţia de atribuire fie din proprie iniţiativă, 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 cunoştinţă a modificărilor operate pînă la noul termen de depunere a ofertelor să rămînă cel puţin 50% din termenul stabilit iniţial.

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 şi alte practici interzise

9.1. Autoritățile contractante şi participanţii la procedurile de achiziții publice vor respecta cele mai înalte standarde ale eticii de conduită în desfăşurarea şi implementarea proceselor de achiziţii, precum şi 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 concurenţă pentru contractul de achiziţie publică sau pe parcursul executării contractului, aceasta:

a. va exclude ofertantul din procedura respectivă de achiziţie prin includerea lui în Lista de interdicţie, 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 achiziţie şi executării contractului nu se permit următoarele acţiuni:

a. promisiunea, oferirea sau darea unei persoane cu funcţie de răspundere, personal sau prin mijlocitor, de bunuri sau servicii, sau a oricărui alt lucru de valoare, pentru a influenţa acţiunile unei alte părţi;

b. orice acţiune sau omisiune, inclusiv interpretare eronată, care, conştient sau din neglijenţă, induce în eroare sau tinde să inducă în eroare o parte pentru obţinerea unui beneficiu financiar sau de altă natură ori pentru a evita o obligaţie;

c. înţelegerea interzisă de lege, între două sau mai multe părţi, realizată în scopul coordonării comportamentului lor la procedurile de achiziţii publice;

d. deteriorarea sau prejudicierea, direct sau indirect, a oricărei părţi sau a proprietăţii acestei părţi, pentru a influenţa în mod necorespunzător acţiunile acesteia;

e. distrugerea intenţionată, falsificarea, contrafacerea sau ascunderea materialelor de evidenţă ale investigării, sau darea unor informaţii false anchetatorilor, pentru a împiedica esenţial o anchetă condusă de către organele de resort în vederea identificării unor practici menţionate la lit. a)-d); precum şi ameninţarea, hărţuirea sau intimidarea oricărei părţi pentru a o împiedica să divulge informaţia cu privire la chestiuni relevante anchetei sau să exercite ancheta.

9.5. Personalul autorităţii contractante are obligaţia de a exclude practicile de corupere în vederea obţinerii beneficiilor personale în legătură cu desfăşurarea procedurii de achiziţii publice.

Secțiunea a-2-a. Criterii de calificare

10. Criterii generale

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

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

10.3. Autoritatea contractantă va aplica criterii și cerințe de calificare numai referitoare la:

a) eligibilitatea ofertantului sau candidatului;
b) capacitatea de exercitare a activității profesionale;
c) capacitatea economică şi financiară;
d) capacitatea tehnică şi/sau profesională;
e) standarde de asigurare a calității;
f) standarde de protecţie 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 achiziţie 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

infracțiuni 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 achiziţie publică, şi respectiv nu este eligibil, orice ofertant care se află în oricare dintre următoarele situaţii:

a. se află în proces de insolvabilitate ca urmare a hotărîrii judecătorești;

b. nu şi-a îndeplinit obligaţiile de plată a impozitelor, taxelor şi contribuţiilor de asigurări sociale către bugetele componente ale bugetului general consolidat, în conformitate cu prevederile legale în Republica Moldova sau în ţara în care este stabilit;

c. a fost condamnat, în ultimii trei ani, prin hotărîrea definitivă a unei instanţe judecătoreşti, pentru o faptă care a adus atingere eticii profesionale sau pentru comiterea unei greşeli în materie profesională;

d. prezintă informaţii false sau nu prezintă informaţiile solicitate de către autoritatea contractantă, în scopul demonstrării îndeplinirii criteriilor de calificare şi selecţie;

e. a încălcat obligaţiile aplicabile în domeniul mediului, muncii şi 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 alţi operatori economici acorduri care vizează denaturarea concurenţei, în cazul în care acest fapt se constată printr-o decizie a organului abilitat în acest sens;

h. se află într-o situaţie 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 interdicţie 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 informaţia necesară pentru constatarea existenţei sau inexistenţei circumstanţelor menționate la punctele IPO11.2 și IPO11.3 din bazele de date disponibile ale autorităţilor publice sau ale părţilor terţe. Dacă acest lucru nu este posibil, autoritatea contractantă are obligaţia de a accepta ca fiind suficient şi relevant pentru demonstrarea faptului că ofertantul/candidatul nu se încadrează în una dintre situaţiile prevăzute menționate la punctele IPO11.2 şi IPO11.3 orice document considerat edificator, din acest punct de vedere, în ţara de origine sau în ţara în care ofertantul este stabilit, cum ar fi certificate, caziere judiciare sau alte documente echivalente emise de autorităţi competente din ţara respectivă.

11.6. În ceea ce priveşte cazurile menţionate la punctul IPO11.3, în conformitate cu legislaţia internă a statului în care sunt stabiliţi ofertanţii, aceste solicitări se referă la persoane fizice şi 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 priveşte ofertantul/candidatul.

11.7. În cazul în care în ţara de origine sau în ţara în care este stabilit ofertantul/candidatul nu se emit documente de natura celor prevăzute la punctul IPO11.4 sau respectivele documente nu vizează toate situaţiile prevăzute la punctele IPO11.2 şi IPO11.3, autoritatea contractantă are obligaţia de a accepta o declaraţie pe propria răspundere sau, dacă în ţara respectivă nu există prevederi legale referitoare la declarația pe propria răspundere, o declaraţie autentică dată în faţa unui notar, a unei autorităţi administrative sau judiciare sau a unei asociaţii profesionale care are competenţe în acest sens.

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

la motivele de excludere, cu excepția cazului în care operatorul economic a fost exclus prin hotărîre 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 ținînd 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 şi financiară

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

a. declaraţii bancare corespunzătoare sau, după caz, dovezi privind asigurarea riscului profesional;
b. rapoarte financiare sau, în cazul în care publicarea acestor rapoarte este prevăzută de legislaţia ţării în care este stabilit ofertantul, extrase de rapoarte financiare;
c. declaraţii 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 informaţiile respective sînt disponibile. În acest ultim caz, autoritatea contractantă are obligaţia de a lua în considerare şi data la care operatorul economic a fost înfiinţat sau şi-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 acordata 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 dispoziţia 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 achiziţii publice de bunuri/servicii, în scopul verificării capacităţii tehnice şi/sau profesionale a ofertanţilor/candidaţilor, autoritatea contractantă are dreptul de a le solicita acestora, în funcţie de specificul, de volumul şi de complexitatea bunurilor/serviciilor ce urmează să fie livrate/prestate şi numai în măsura în care aceste informaţii sînt relevante pentru îndeplinirea contractului şi nu sînt disponibile în bazele de date ale autorităţilor publice sau ale părţilor terţe, următoarele:

a) lista principalelor bunuri/servicii similare livrate/prestate în ultimii 3 ani, conţinînd valori, perioade de livrare/prestare, beneficiari, indiferent dacă aceştia din urmă sînt autorităţi contractante sau clienţi privaţi. 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 obţinerii unei certificări/confirmări din partea acestuia, demonstrarea furnizărilor de bunuri sau prestărilor de servicii se realizează printr-o declaraţie a operatorului economic;

b) declaraţia referitoare la echipamentele tehnice şi la măsurile aplicate în vederea asigurării calităţii, precum şi, dacă este cazul, la resursele de studiu şi cercetare;

c) informaţii referitoare la personalul/organismul tehnic de specialitate de care dispune sau al cărui angajament de participare a fost obţinut de către ofertant/candidat, în special pentru asigurarea controlului calităţii;

d) informaţii referitoare la studiile, pregătirea profesională şi calificarea personalului de conducere, precum şi ale persoanelor responsabile pentru îndeplinirea contractului, dacă acestea nu reprezintă factori de evaluare stabiliţi de autoritatea contactantă;

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

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

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

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

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

14.3. În cazul prevăzut la punctul IPO14.2, ofertantul/candidatul are obligaţia de a dovedi susţinerea 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 dispoziţia ofertantului/candidatului resursele financiare invocate.

14.4. Persoana care asigură susţinerea financiară trebuie să îndeplinească criteriile de selecţie relevante și nu trebuie să se afle în niciuna dintre situaţiile 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 calităţii.

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 calităţii, aceasta trebuie să se raporteze la sistemele de asigurare a calităţii, 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 recunoaşterii reciproce, autoritatea contractantă are obligaţia de a accepta certificatele echivalente emise de organismele stabilite în statele membre ale Uniunii Europene. În cazul în care operatorul economic nu deţine un certificat de calitate astfel cum este solicitat de autoritatea contractantă, aceasta din urmă are obligaţia de a accepta orice alte certificări prezentate de operatorul economic respectiv, în măsura în care acestea confirmă asigurarea unui nivel corespunzător al calităţii.

16. Standarde de protecţie 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 protecţie a mediului, aceasta trebuie să se raporteze:

a) fie la Sistemul Comunitar de Management de Mediu şi Audit (EMAS);

b) fie la standarde de gestiune ecologică bazate pe seriile de standarde europene sau internaţionale în domeniu, certificate de organisme conforme cu legislaţia Uniunii Europene ori cu standardele europene sau internaţionale privind certificarea.

16.2. În conformitate cu principiul recunoaşterii reciproce, autoritatea contractantă are obligaţia de a accepta certificatele echivalente emise de organismele stabilite în statele membre ale Uniunii Europene. În cazul în care operatorul economic nu deţine un certificat de mediu astfel cum este solicitat de autoritatea contractantă, aceasta din urmă are obligaţia de a accepta orice alte certificări prezentate de operatorul economic respectiv, în măsura în care acestea confirmă asigurarea unui nivel corespunzător al protecţiei 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 exceptia cazurilor prevazute la art.32 alin.(7) şi (11) din Legea nr. 131/2015.

19. Documente pentru demonstrarea conformităţii bunurilor/serviciilor

19.1. Pentru a stabili conformitatea bunurilor/serviciilor cu cerinţele documentelor de atribuire, ofertantul desemnat cîştigător la procedura de achiziţie în cauză, va prezenta, la solictarea autorităţii contractante, dovezi documentare ce atestă faptul că bunurile/serviciile se conformează condiţiilor de livrare/prestare, specificaţiilor tehnice şi standardelor specificate în CAPITOLUL IV.

19.2. Pentru a demonstra conformitatea tehnică a bunurilor/serviciilor propuse, cantităţilor propuse şi a termenelor de livrare/prestare, ofertantul va completa Formularul Specificaţii tehnice **(F4.1)** și Specificaţii de preț **(F4.2)**. De asemenea, ofertantul va include documentație de specialitate, desene, extrase din cataloage şi 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 anunţul de participare şi în **FDA** punctul **3.1** că permite sau solicită depunerea de oferte alternative cu precizarea în documentaţia de atribuire a cerinţelor minime obligatorii pe care operatorii economici trebuie să le respecte, precum şi orice alte cerinţe specifice pentru prezentarea ofertelor alternative. În cazul în care în documentația de atribuire nu este specificat explicit că autortiatea contractantă permite sau solicită depunerea de oferte alternative, aceasta din urmă nu are dreptul de a lua în considerare ofertele alternative.

21. Garanţia 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 Garanţie pentru ofertă **(F3.2)**.

21.2. Garanţia pentru ofertă va fi corespunzător cuantumului specificat în **FDA** punctul **3.3**, în lei moldoveneşti, şi va fi:

a) în formă de garanţie bancară de la o instituţie 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 autorităţii contractante; sau

c) alte forme acceptate de autoritatea contractantă, specificate în **FDA** punctul **3.2**.

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

21.4. Garanţia pentru ofertă a ofertanţilor necîştigători va fi restituită imediat de la producerea oricărui din următoarele evenimente:

a) expirarea termenului de valabilitate a garanţiei pentru ofertă;

b) încheierea unui contract de achiziţii publice şi depunerea garanţiei de bună execuţie a contractului, dacă o astfel de garanţie este prevăzută în documentaţia de atribuire;

c) suspendarea procedurii de achiziţie fără încheierea unui contract de achiziţii publice;

d) retragerea ofertei înainte de expirarea termenului de depunere a ofertelor, în cazul în care documentaţia de atribuire nu prevede inadmisibilitatea unei astfel de retrageri.

21.5. Garanţia pentru ofertă va fi reţinută dacă:

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

b) ofertantul cîştigător refuză:

- să depună Garanţia de bună execuţie conform punctului IPO42;
- să semneze contractul conform punctului IPO43.

21.6. Garanţia pentru ofertă prezentată de Asociaţie trebuie să fie în numele Asociaţiei care depune oferta.

22. Preţuri

22.1. Preţurile indicate de către ofertant în Formularul ofertei **(F3.1)** şi în Specificaţiile de preț **(F4.2)** se vor conforma cerinţelor specificate în punctul IPO22.

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

22.3. Preţul 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 şi alţi termeni similari, vor fi supuşi regulilor prevăzute în ediţia curentă a Incoterms, publicată de către Camera Internaţională de Comerţ, după cum este menţionat în **FDA** punctul **3.4**.

22.5. Preţurile vor fi indicate după cum este arătat în Specificaţiile 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 rămîne 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 excepţionale, înainte de expirarea perioadei de valabilitate a ofertei, autoritatea contractantă poate solicita ofertanţilor să extindă perioada de valabilitate a ofertelor. Solicitarea şi răspunsul la solicitarea de prelungire a valabilității ofertei vor fi publicate în SIA „RSAP”. În cazul în care se cere o garanţie pentru ofertă în cadrul procedurii de achiziție publică, conform prevederilor punctului IPO23, operatorul economic va extinde corespunzător valabilitatea garanţiei pentru ofertă. Un ofertant poate refuza solicitarea de extindere fără a pierde garanţia pentru ofertă. Ofertanţilor ce acceptă solicitarea de extindere nu li se va cere şi nu li se va permite să modifice ofertele.

24. Valuta ofertei

24.1. Preţurile pentru bunurile/serviciile solicitate vor fi indicate în lei moldoveneşti, cu excepţia 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 exceptia cazurilor prevazute la art.32 alin.(7) şi (11) din Legea nr. 131/2015.

Secțiunea a-4-a. Depunerea și deschiderea ofertelor

26. Depunerea ofertelor

26.1. Oferta , scrisă şi semnată, se prezintă în fromat electronic în conformitate cu cerinţele expuse în documentaţia de atribuire, utilizind SIA „RSAP”, cu exceptia cazurilor prevazute la art.32 alin.(7) şi (11) din Legea nr. 131/2015. Autoritatea contractantă eliberează operatorului economic, în mod obligatoriu, o recipisă în care indică data şi ora recepţionării ofertei sau confirmă recepţionarea acesteia în cazurile în care oferta a fost depusă prin mijloace electronice. Prezentarea ofertei presupune depunerea într-un set comun a ofertei de preţuri, a sepcificației tehnice, a **DUAE** și a garanţiei 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, prevăzînd timp suficient pentru a depune oferta în termenii stabiliți.

27. Termenul limită de depunere a ofertelor

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

28. Oferte întîrziate

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) şi (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 şi restituite ofertantului, fără a fi deschise.

29. Modificarea, substituirea şi retragerea ofertelor

29.1. În cazul în care documentaţia 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 garanţiei 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 şi 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 achiziţii publice pentru bunuri şi servicii prin cererea ofertelor de preţuri este obligatoriu precedată de licitaţia 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. Licitația 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 rundei 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. Licitația electronică va lua sfîrșit 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 ofertat, fără a se permite însă modificarea acestuia.

Secțiunea a-6-a. Evaluarea și compararea ofertelor

31. Confidenţialitate

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

32. Clarificarea ofertelor

32.1. Autoritatea contractantă poate, la necesitate, să ceară oricăruia dintre ofertanţi o clarificare a ofertei acestora, pentru a facilita examinarea, evaluarea și compararea ofertelor. Nu vor fi solicitate, oferite sau permise schimbări în preţurile sau în conţinutul ofertei, cu excepţia 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 autorităţii contractante de a reconfirma datele de calificare pentru încheierea contractului, oferta i se respinge şi se selectează o altă ofertă cîştigătoare 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 conformităţii ofertelor

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

33.2. Se consideră conformă cerinţelor oferta care corespunde tuturor termenilor, condiţiilor şi specificaţiilor din documentele de atribuire, neavînd abateri esenţiale sau avînd doar abateri neînsemnate, erori sau omiteri ce pot fi înlăturate fără a afecta esenţa ofertei. O abatere se va considera ca fiind neînsemnată dacă:

a) nu afectează în orice mod substanţial sfera de acţiune, calitatea sau performanţa bunurilor/serviciilor specificate în contract;

b) nu limitează în orice mod substanţial drepturile autorităţii contractante sau obligaţiile ofertantului conform contractului;

c) nu ar afecta într-un mod inechitabil poziţia competitivă a altor ofertanţi ce prezintă oferte conforme cerinţelor.

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

34. Neconformităţi, erori şi omiteri

34.1. Autoritatea contractantă are dreptul să considere oferta conformă cerinţelor dacă aceasta conţine abateri neînsemnate de la prevederile documentelor de atribuire, erori sau omiteri ce pot fi înlăturate fără a afecta esenţa ei. Orice deviere de acest fel se va exprima cantitativ, în măsura în care este posibil, şi se va lua în considerare la evaluarea şi 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 şi compararea ofertelor se efectuează fără participarea ofertanţilor şi a altor persoane neautorizate. Autoritatea contractantă va examina ofertele pentru a confirma faptul că toate documentele prevăzute în punctul IPO18 au fost prezentate şi pentru a determina caracterul complet al fiecărui document depus.

35.2. Autoritatea contractantă stabileşte oferta/ofertele cîştigătoare aplicînd criteriul de atribuire şi factorii de evaluare prevăzuţi în documentaţia de atribuire, utilizînd instrumentele de evaluare din cadrul SIA „RSAP”, cu exceptia cazurilor prevazute la art.32 alin.(7) şi (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 minuţioasă a documentelor de calificare ale ofertantului, inclusiv DUAE, incluse în ofertă conform prevederilor punctului IPO18, clarificărilor posibile conform punctului IPO32, precum şi 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 capacităţilor acelui ofertant în executarea contractului.

37. Descalificarea ofertantului

37.1. Autoritatea contractantă va descalifica ofertantul care depune documente ce conţin informaţii false, cu scopul calificării, sau derutează ori face reprezentări neadevărate pentru a demonstra corespunderea sa cerinţelor de calificare. În cazul în care acest lucru este dovedit, autoritatea contractantă poate înainta o solicitare către Agenţia Achiziţii Publice cu privire la înscrierea ofertantului respectiv în Lista de interdicţie a operatorilor economici.

37.2. Lista de interdicţie a operatorilor economici reprezintă un înscris oficial şi este întocmită actualizată şi ţinută de către Agenţia Achiziţii Publice conform prevederilor articolului 25 din Legea nr. 131/2015, cu scopul de a limita participarea operatorilor economici la procedurile de achiziţie publică

37.3. Ofertantul poate fi descalificat în cazul în care este insolvabil, în privinţa lui a fost iniţiată procedura de sechestrare a patrimoniului, este în faliment sau în proces de lichidare sau dacă activităţile ofertantului sînt suspendate ori există un proces de judecată privind oricare dintre cele menţionate.

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

37.5. Ofertantul este descalificat pentru neachitarea impozitelor şi altor plăţi obligatorii în conformitate cu legislaţia ţării în care el este rezident. Autoritatea contractantă va solicita ofertanţilor să demonstreze împuternicirea de a încheia contractele de achiziţii publice şi componenţa fondatorilor şi a persoanelor afiliate.

37.6. Autoritatea contractantă descalifică ofertantul dacă constată că acesta este inclus în Lista de interdicţie 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 obligaţia de a comunica prin SIA „RSAP” sau prin alte mijloace de comunicare în cazul în care autoritatea contractantă desfăşoară proceduri în baza art. 32 alin.(7) şi (11) din Legea nr. 131/2015, tuturor participanţilor la procedura de achiziţie publică, în cel mult 3 zile de la data anulării, atît încetarea obligaţiilor pe care aceştia şi le-au creat prin depunerea de oferte, cît şi 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.** acelui ofertant a cărui ofertă a fost apreciată potrivit criteriilor stabilite precum şi altor condiţii şi cerinţelor din documentele de atribuire, cu condiţia ca şi ofertantul să fie calificat pentru executarea contractului.

40. Dreptul autorităţii contractante de a modifica cantităţile în timpul adjudecării

40.1. La momentul adjudecării contractului, autoritatea contractantă are posibilitatea de a micşora cu acordul operatorului economic, cantitatea de bunuri/servicii, în cazul în care suma contractelor este mai mare decît valoare estimată a achiziţiei, specificate iniţial în CAPITOLUL IV pentru a se putea încadra în mijloacele financiare alocate, însă fără a efectua vreo schimbare în preţul unitar sau în alţi termeni şi condiţii ale ofertei şi ale documentelor de atribuire.

41. Înştiinţarea 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 necîștigători 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 tîrziu de data expirării Garanției pentru ofertă (dacă s-a cerut), ofertantul cîștigător 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 cîștigător 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 cărui 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 cîștigător Formularul contractului de bunuri **(F5.1)** sau Formularul contractului de servicii **(F5.2)** completat și toate celelalte documente componente ale contratului.

43.2. Ofertantul cîștigător 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 căruia 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. Contestațiile se vor depune direct la Agenția Națională de Soluționare a Contestațiilor. Toate contestațiile vor fi depuse, examinate și soluționate în modul stabilit de Legea nr. 131/2015.

44.3. Operatorul economic, în termen de pînă 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 Contestațiilor o contestație argumentată a acțiunilor, a deciziei ori a procedurii aplicate de autoritatea contractantă.

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

CAPITOLUL II
FIȘA DE DATE A ACHIZIȚIEI (FDA)

Următoarele date specifice referitoare la bunutilr/serviciile solicitate vor completa, suplimenta sau ajusta prevederile CAPITOLULUI I. În cazul unei discrepanţe 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.P. „Centrul de Tehnologii Informaționale în Finanțe” IDNO 1005600036924***
1.2.	Obiectul achiziției:	***Servicii de mentenanță a Sistemului Informațional de Evidență Contabilă 1C, Contabilitate versiune 8.3***
1.3.	Numărul procedurii de achiziție:	***Nr.: MTender ID ocds-b3wdp1-MD-1616657521500***
1.4.	Tipul obiectului de achiziție:	***Bunuri***
1.5.	Codul CPV:	***48761000-0***
1.6.	Sursa alocațiilor bugetare/banilor publici și perioada bugetară:	***Surse proprii, 2021***
1.7.	Administratorul alocațiilor bugetare:	***I.P. „Centrul de Tehnologii Informaționale în Finanțe”***
1.8.	Partenerul de dezvoltare (după caz):	***Nu se aplică***
1.9.	Denumirea cumpărătorului, IDNO:	***I.P. „Centrul de Tehnologii Informaționale în Finanțe” IDNO 1005600036924***
1.10.	Destinatarul bunurilor/serviciilor, IDNO:	***I.P. „Centrul de Tehnologii Informaționale în Finanțe” IDNO 1005600036924***
1.11.	Limba de comunicare:	***Limba de stat***
1.12.	Locul/Modalitatea de transmitere a clarificărilor referitor la documentația de atribuire	***Prin intermediul SIA „RSAP”***
1.13.	Contract de achiziție rezervat atelierelor protejate	***Nu se aplică***
1.14.	Tipul contractului:	***Vînzare-cumpărare***
1.15.	Condiții speciale de care depinde îndeplinirea contractului**:**	***Nu se aplică***

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) si sa 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 ofertate trebuie sa prelungească licențele existente pentru 12 luni.

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 si Android.
3. Protecție și securitate de tip „sandboxing” pentru serverele si 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 urma nu va necesita o licență suplimentară pentru sistemul de operare, iar imaginea de tip template va fi posibil de a fi importata în următoarele platforme de virtualizare: VMware vSphere, Citrix XenServe, Microsoft Hyper-V, Red Hat Enterprise Virtualization, KVM, Oracle VM.

Consola de management va fi oferita 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 in limba romana. Interfața agentului care se instalează pe stații de lucru si servere, va fi in limba romana.

Cerințe 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. 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 si 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.
8. Permită crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programat, stocata 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 si 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. Permită 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. Permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea.
13. Permită crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul va putea descarcă pachetele pentru protecția stațiilor si serverelor pe care rulează sistemul de operare Windows, Linux si Mac.

Politici:

Produsul trebuie să:
1. Permită 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. Permită 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. 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 prezinta 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 si detaliile ca format .csv.
7. Includă un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise si 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 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.

Protecție stații și servere fizice si 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 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,

dezinfecție, 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 maliții os, 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: 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 in mai multe moduri:
- prin descărcarea directa a pachetului pe stația pe care se va face instalarea;
- prin instalarea la distanta, 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 si/sau virtuale), servere (fizice si/sau virtuale), exchange;

Caracteristici și funcționalități principale ale modulului antivirus

Produsul trebuie sa 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 virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansata 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 pana la 16 nivele de profunzime pentru scanarea in 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 in 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.

Protecția datelor:

1. Produsul trebuie să permite 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, violenta, pornografie etc).

Controlul aplicațiilor:

Pentru administrare și inventariere eficientă produsul trebuie 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 subprocese) 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 si Google Play.
5. Să poată întreprinde următoarele acțiuni: blocarea dispozitivului; deblocarea dispozitivului; ștergerea datelor si 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 sa 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 si 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 si intervale orare a accesului la anumite pagini de internet; crearea unor excepții pentru blocarea sau permiterea accesului către anumite pagini de internet.
10. Includă posibilitatea de configurare profilurile acces pagini de internet pentru sistemul de operare iOS cu opțiuni de activare sau dezactivare a: utilizarii browser-ului Safari; opțiunii de completare automata a informațiilor; alertării utilizatorului în cazul accesării unor pagini frauduloase; Javascript; Pop-up-urilor; Cookie-uri.

<u>Protecție și securitate pentru serverele de mail Microsoft Exchange</u>

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 si 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 (dezinfectare, 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 baza de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automata 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 şi menţinere de la producător:

1. Pentru soluția ofertată 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 in limba romana sau rusă din partea partenerului;
3. Ofertantul va prezenta autorizarea de la producător pentru produsul și suportul livrat;
4. Ofertantul trebuie sa posede minim 2 persoane tehnice calificate pe produsul ofertat;
5. Se va oferi manual de instalare si administrare a produsului ofertat in limba romana si engleza.
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 semănării contractului.

3. Pregătirea ofertelor

3.1.	Oferte alternative:	***nu vor fi acceptate***
3.2.	Garanţia pentru ofertă:	*Oferta va fi însoţită de o Garanţie pentru ofertă (emisă de o bancă comercială) conform formularului F3.2 din secţiunea a 3-a – Formulare pentru depunerea ofertei;* *Sau, prin transfer la contul autorităţii contractante, conform următoarelor date bancare:* *Beneficiarul plăţii:* ***Instituția Publică "Centrul de Tehnologii Informaționale în Finanțe"*** - Cod IBAN: MD86TRPCCC518430A01338AA - Codul băncii:TREZMD2X - Banca: Ministerul Finanțelor – Trezoreria de Stat - Cod fiscal: 1005600036924 - Cod TVA 7800104 *cu nota "Pentru garanţia pentru ofertă la procedura de achiziţie publică nr. MTender ID ocds-b3wdp1-MD-1616657521500*
3.3.	Garanţia pentru ofertă va fi în valoare de:	***1% din valoarea ofertei fără TVA.***
3.4.	Ediţia aplicabilă a Incoterms și termenii comerciali acceptați vor fi (după caz):	***INCOTERMS 2010 DDP***
3.5.	Termenul de livrare:	***licențele vor fi prelungite din data de 10.05.2020, pe un termen de 12 luni***

3.6.	Locul livrării bunurilor:	***mun.Chișinău, str. C.Tănase 7***
3.7.	Metoda şi condiţiile de plată vor fi:	**Achitarea va fi efectuată utilizînd sistemul „e-factura" în termen de 15 (cincisprezece) zile bancare din data facturării.**
3.8.	Perioada valabilităţii ofertei va fi de:	*45 zile*
3.9.	Ofertele în valută străină:	***nu se acceptă***

4. Depunerea și deschiderea ofertelor

4.1	Locul/Modalitatea de **depunere a ofertelor**, este:	*SIA „RSAP"*
4.2.	**Termenul limită** de depunere a ofertelor este:	*conform datelor SIA „RSAP"*
4.3.	Persoanele autorizate să asiste la deschiderea ofertelor (cu excepţia cazului cînd ofertele au fost depuse prin SIA "RSAP").	*Ofertanţii sau reprezentanţii acestora au dreptul să participe la deschiderea ofertelor, cu excepţia cazului cînd ofertele au fost depuse prin SIA „RSAP"*

5. Evaluarea și compararea ofertelor

5.1.	Preţurile ofertelor depuse în diferite valute vor fi convertite în:	***Ofertele în valută străină: nu se acceptă.***
	Sursa ratei de schimb în scopul convertirii:	-
	Data pentru rata de schimb aplicabilă va fi:	-
5.2.	Modalalitatea de efectuare a evaluării:	***Evaluarea va fi efectuată: pe lot.***

5.3.	Factorii de evaluarea vor fi următorii:	***corespunderea cerințelor tehnice la prețul cel mai scăzut.***

6. Adjudecarea contractului

6.1.	Criteriul de evaluare aplicat pentru adjudecarea contractului va fi:	***După criteriul: prețul cel mai scăzut.***
6.2.	Suma Garanţiei de bună execuţie (se stabileşte procentual din preţul contractului adjudecat):	***3 %***
6.3.	Garanţia de bună execuţie a contractului:	*Garanția de buna execuție (emisă de o bancă comercială) conform formularului F3.4* *Sau,* *prin transfer la contul autorității contractante, conform următoarelor date bancare:* *Beneficiarul plății:* ***Instituția Publică "Centrul de Tehnologii Informaționale în Finanțe"*** - *Cod IBAN: MD86TRPCCC518430A01338AA* - *Codul băncii:TREZMD2X* - *Banca: Ministerul Finanțelor – Trezoreria de Stat* - *Cod fiscal: 1005600036924* - *Cod TVA 7800104* *cu nota "Pentru garanția pentru ofertă la procedura de achiziție publică nr. MTender ID ocds-b3wdp1-MD-1616657521500*
6.4.	Forma de organizare juridică pe care trebuie să o ia asocierea grupului de operatori economici cărora li s-a atribuit contractul	a) Societate pe acţiuni b) Societate cu răspundere limitată c) Altele _____
6.5.	Numărul maxim de zile pentru semnarea şi prezentarea contractului către autoritatea contractantă, de la remiterea acestuia spre semnare:	*15 zile*

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.

Digitally signed by Muntean Vadim
Date: 2021.03.25 10:58:17 EET
Reason: MoldSign Signature
Location: Moldova

Conducătorul grupului
de lucru pentru achiziții: _____ Vadim MUNTEAN

CAPITOLUL III
FORMULARE PENTRU DEPUNEREA OFERTEI

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

Formular	Denumirea
F3.1	Formularul ofertei
F3.2	Garanţia pentru ofertă – formularul garanţiei bancare
F3.3	Garanţie de bună execuţie

Formularul ofertei (F3.1)

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

Data depunerii ofertei: „___" _____ 20__

Procedura de achiziţie Nr.: _____

Anunţ de participare Nr.: _____

Către: _____

[numele deplin al autorităţii contractante]

_____ declară că:

[denumirea ofertantului]

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

[introduceţi numărul şi data fiecărei modificări, dacă au avut loc]

b) _____ se angajează să

[denumirea ofertantului]

presteze, în conformitate cu documentele de atribuire şi condiţiile stipulate în specificaţiile tehnice şi preț, următoarele servicii _____ _____.

[introduceţi o descriere succintă a serviciilor]

c) Suma totală a ofertei fără TVA constituie:

_____.

[introduceţi preţul pe loturi (unde e cazul) şi totalul ofertei în cuvinte şi cifre, indicînd toate sumele şi valutele respective]

d) Suma totală a ofertei cu TVA constituie:

_____.

[introduceţi preţul pe loturi (unde e cazul) şi totalul ofertei în cuvinte şi cifre, indicînd toate sumele şi valutele respective]

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

f) În cazul acceptării prezentei oferte, _____

[denumirea ofertantului]

se angajează să obţină o Garanţie de bună execuţie în conformitate cu **FDA6**, pentru executarea corespunzătoare a contractului de achiziţie publică.

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

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

Semnat:_____

[semnătura persoanei autorizate pentru semnarea ofertei]

Nume:_____

În calitate de: _____

[funcţia oficială a persoanei ce semnează formularul ofertei]

Ofertantul: _____

Adresa: _____

Data: "___" _____ 20__

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

[Banca emitentă va completa acest formular de garanţie bancară în conformitate cu instrucţiunile indicate mai jos. Garanţia bancară se va imprima pe foaie cu antetul băncii, pe hîrtie specială protejată.]

_____
[Numele băncii şi adresa oficiului sau a filialei emitente]

Beneficiar: _____
[numele şi adresa autorităţii contractante]

Data: "___" _____ 20__

GARANŢIE 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 achiziţiei]

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 depăşesc în total suma de:

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

la primirea de către noi a primei solicitări din partea Dvs. în scris, însoţite de o declaraţie în care se specifică faptul că Ofertantul încalcă una sau mai multe dintre obligaţiile sale referitor la condiţiile ofertei, şi anume:

a) şi-a retras oferta în timpul perioadei valabilităţii ofertei sau a modificat oferta după expirarea termenului-limită de depunere a ofertelor; sau
b) fiind anunţat de către autoritatea contractantă, în perioada de valabilitate a ofertei, despre adjudecarea contractului: (i) eşuează sau refuză să semneze formularul contractului; sau (ii) eşuează sau refuză să prezinte garanţia de bună execuţie, dacă se cere conform condiţiilor procedurii de achiziţie, ori nu a executat vreo condiţie specificată în documentele de atribuire, înainte de semnarea contractului de achiziţie.

Această garanţie va expira în cazul în care ofertantul devine ofertant cîştigător, la primirea de către noi a copiei înştiinţării privind adjudecarea contractului şi în urma emiterii Garanţiei de bună execuţie eliberată către Dvs. la solicitarea Ofertantului.

Prezenta garanţie este valabilă pînă la data de "___" _____ 20__.

_____
[semnătura autorizată a băncii]

Garanţie de bună execuţie (F3.3)

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

Data: "___" _____ 20__

Procedura de achiziţie Nr.: _____

Oficiul Băncii: _____
[introduceţi numele complet al garantului]

Beneficiar: _____
[introduceţi numele complet al autorităţii contractante]

GARANŢIA DE BUNĂ EXECUŢIE
Nr. _____

Noi, *[introduceţi numele legal şi adresa băncii],* am fost informaţi că firmei *[introduceţi numele deplin al Furnizorului/Prestatorului]* (numit în continuare „Furnizor/Prestator") i-a fost adjudecat Contractul de achiziţie publică de livrare/prestare _____ [*obiectul achiziţiei, descrieţi bunurile/serviciile*] conform invitaţiei la procedura de achiziţie nr. din _____. 201_ [*numărul şi data procedurii de achiziţie*] (numit în continuare „Contract").

Prin urmare, noi înţelegem că Furnizorul/Prestatorul trebuie să depună o Garanţie de bună execuţie 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 depăşeşte *[introduceţi suma(ele) în cifre şi cuvinte]* la primirea primei cereri în scris din partea Dvs., prin care declaraţi că Furnizorul/Prestatorul nu îndeplineşte una sau mai multe obligaţii conform Contractului, fără discuţii sau clarificări şi fără necesitatea de a demonstra sau arăta temeiurile sau motivele pentru cererea Dvs. sau pentru suma indicată în aceasta.

Această Garanţie va expira nu mai tîrziu de *[introduceţi numărul]* de la data de *[introduceţi luna] [introduceţi anul]*,[1] şi orice cerere de plată ce ţine de aceasta trebuie recepţionată de către noi la oficiu pînă la această dată inclusiv.

[semnăturile reprezentanţilor autorizaţi ai băncii şi ai Furnizorului/Prestatorului]

[1] *Autoritatea contractantă trebuie să ţină cont de situaţiile cînd, în cazul unei extinderi a perioadei de executare a Contractului, autoritatea contractantă va avea nevoie să ceară o extindere şi a acestei garanţii de la bancă. O astfel de cerere trebuie să fie întocmită în scris şi trebuie făcută înainte de expirarea datei stabilite în garanţie. În procesul pregătirii acestei Garanţii, autoritatea contractantă ar putea lua în considerare adăugarea următorului text în formular, la sfîrşitul penultimului paragraf: „Noi sîntem de acord cu o singură extindere a acestei Garanţii pentru o perioadă ce nu depăşeşte [şase luni] [un an], ca răspuns al cererii în scris a autorităţii contractante pentru o astfel de extindere, şi o astfel de cerere urmează a fi prezentată nouă înainte de expirarea prezentei garanţii."*

CAPITOLUL IV
SPECIFICAȚII TEHNICE ȘI DE PREȚ

Următoarele tabele şi formulare vor fi completate de către ofertant şi 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	Specificaţii tehnice
F4.2	Specificații de preț

Specificaţii 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**	**Ţara de origine**	**Producătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standard de referinţă**
1	2	3	4	5	6	7	8
48761000-0	Pachet software antivirus				Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST) si sa fie prezent în mențiunile Gartner. Satisfacerea necesităților minime va constitui500 licențe (workstation PC, mailboxes), și 100 licențe (VDI/VS/Server), în scopul managementului centralizat pentru dispozitive. Licențele ofertate trebuie sa prelungească licențele existente pentru 12 luni. 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 si Android. 3. Protecție și securitate de tip „sandboxing” pentru serverele si 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 urma nu va necesita o licență suplimentară pentru sistemul de operare, iar imaginea de tip template va fi posibil de a fi importata în următoarele platforme de virtualizare: VMware vSphere, Citrix XenServe, Microsoft Hyper-V, Red Hat Enterprise Virtualization, KVM, Oracle VM. Consola de management va fi oferita 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 in limba romana. Interfața agentului care se instalează pe stații de lucru si servere, va fi in limba romana. Cerințe 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. 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 si 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.		

					8. Permită crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programat, stocata 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 si 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. Permită 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. Permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea. 13. Permită crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul va putea descarcă pachetele pentru protecția stațiilor si serverelor pe care rulează sistemul de operare Windows, Linux si Mac. Politici: Produsul trebuie să: 1. Permită 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. Permită 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. 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 prezinta 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 si detaliile ca format .csv. 7. Includă un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise si 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 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. Protecție stații și servere fizice si 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 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, dezinfecție, 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:		

					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 in mai multe moduri: - prin descărcarea directa a pachetului pe stația pe care se va face instalarea; - prin instalarea la distanta, 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 si/sau virtuale), servere (fizice si/sau virtuale), exchange; Caracteristici și funcționalități principale ale modulului antivirus Produsul trebuie sa 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 virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansata 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 pana la 16 nivele de profunzime pentru scanarea in 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 in 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. Protecția datelor: 1. Produsul trebuie să permite 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, violenta, pornografie etc). Controlul aplicațiilor: Pentru administrare și inventariere eficientă produsul trebuie 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 subprocese) 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 si Google Play.		

					5. Să poată întreprinde următoarele acțiuni: blocarea dispozitivului; deblocarea dispozitivului; ștergerea datelor si 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 sa 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 si 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 si intervale orare a accesului la anumite pagini de internet; crearea unor excepții pentru blocarea sau permiterea accesului către anumite pagini de internet. 10. Includă posibilitatea de configurare profilurile acces pagini de internet pentru sistemul de operare iOS cu opțiuni de activare sau dezactivare a: utilizarii browser-ului Safari; opțiunii de completare automata 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 si 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 (dezinfectare, 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 baza de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automata 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 menținere de la producător: 1. Pentru soluția ofertată 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 in limba romana sau rusă din partea partenerului; 3. Ofertantul va prezenta autorizarea de la producător pentru produsul și suportul livrat; 4. Ofertantul trebuie sa posede minim 2 persoane tehnice calificate pe produsul ofertat; 5. Se va oferi manual de instalare si administrare a produsului ofertat in limba romana si engleza. 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 semănării 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**	**Canti-tatea**	**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

Contract-model Servicii (F5.2)

A C H I Z I Ţ I I P U B L I C E

C O N T R A C T 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 *Părţi*, au încheiat prezentul Contract referitor la următoarele:

a. Achiziţionarea 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 părţi componente şi integrale ale Contractului:
   a) Specificaţia tehnică și de preț
   b) *Garanție de bună execuție a contractului*
c. Prezentul Contract va predomina asupra tuturor altor documente componente. În cazul unor discrepanţe sau inconsecvenţe între documentele componente ale Contractului, documentele vor avea ordinea de prioritate enumerată mai sus.
d. În calitate de contravaloare a plăţilor care urmează a fi efectuate de Cumpărător, Vînzătorul se obligă prin prezenta să livreze Cumpărătorului Bunurile şi să înlăture 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 şi a înlăturării defectelor lor, preţul Contractului sau orice altă sumă care poate deveni plătibilă conform prevederilor Contractului în termenele şi modalitatea stabilite de Contract.

1. OBIECTUL CONTRACTULUI

1.1. În conformitate cu prezentul Contract, Vînzătorul 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 Vînzător 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 Vînzătorului, 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 Vînzător 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 Vînzătorul 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 Vînzător, 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, Vînzătorul 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 obligațiunilor 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 obligațiunile sale din cauza impedimentului justificator va notifica cealaltă parte despre survenirea acestui impediment și efectele lui asupra capacității de a executa, asupra executării obligațiunilor 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 SANCȚIUNI

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 _____ _____ L.Ș.	**Director** **Vitalie COCEBAN** _____ 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.