

**DOCUMENTAȚIA de ATRIBUIRE
pentru realizarea achizițiilor publice de bunuri**

Obiectul achiziției: *Pachete software aferente securității
informaționale*

Cod CPV: 48000000-8; 72200000-7

Autoritatea contractantă: *Banca Națională a Moldovei*

Procedura de achiziție: *Licitație deschisă*

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

Secțiunea 1. Dispoziții generale

1. Scopul procedurii de achiziție

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

2. Principiile care stau la baza atribuirii contractului de achiziție

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

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

3. Sursa de finanțare

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

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

4. Participanții la licitație

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

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

5. Cheltuielile de participare la procedura de achiziție

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

5.2. La depunerea ofertelor, operatorul economic, după caz, va achita o taxă. Modul de achitare a taxei menționate, precum și quantumul 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 licitației

6.1. Oferta, Documentul Unic de Achiziții European (în continuare **DUAE**), documentele de

atribuire și toată corespondența dintre ofertant și autoritatea contractantă vor fi întocmite în limba de stat. Documentele justificative și literatura de specialitate tipărită, care fac parte din ofertă, pot fi în altă limbă, cu condiția ca acestea să fie însoțite de o traducere exactă a fragmentelor relevante în limba de stat.

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

7. Secțiunile Documentelor de atribuire

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

CAPITOLUL I. Instrucțiuni pentru ofertanți

CAPITOLUL II. Fișa de date a achiziției

CAPITOLUL III. Formulare pentru depunerea ofertei

CAPITOLUL IV. Specificații tehnice și de preț.

CAPITOLUL V. Formularul de contract

8. Clarificarea și modificarea documentelor de atribuire

8.1. Participantul care solicită clarificări asupra documentelor de atribuire va contacta autoritatea contractantă în scris, prin mijloace electronice de comunicare. Autoritatea contractantă va răspunde în scris, prin mijloace electronice de comunicare la orice cerere de clarificare, înainte de termenul-limită pentru depunerea ofertelor.

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

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

9. Practicile de corupere și alte practici interzise

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

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

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

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

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

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

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

b. orice acțiune sau omisiune, inclusiv interpretare eronată, care, conștient sau din

neglijență, induce în eroare sau tinde să inducă în eroare o parte pentru obținerea unui beneficiu financiar sau de altă natură ori pentru a evita o obligație;

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

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

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

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

Secțiunea a-2-a. Criterii de calificare

10. Criterii generale

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

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

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

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

11. Eligibilitatea ofertantului sau candidatului

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

11.2. Va fi exclus de la procedura de atribuire a contractului de achiziții publice orice ofertant sau candidat despre care se confirmă că, în ultimii 5 ani, a fost condamnat, prin hotărârea definitivă a unei instanțe judecătorești, pentru participare la activități ale unei organizații sau grupări criminale, pentru corupție, pentru fraudă și/sau pentru spălare de bani, pentru infracțiuni de terorism sau 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 achiziție publică, și respectiv nu este eligibil, orice ofertant care se află în oricare dintre următoarele situații:

- a. se află în proces de insolabilitate ca urmare a hotărârii judecătorești;
- b. nu și-a îndeplinit obligațiile de plată a impozitelor, taxelor și contribuțiilor de asigurări sociale către bugetele componente ale bugetului general consolidat, în conformitate cu prevederile legale în Republica Moldova sau în țara în care este stabilit;
- c. a fost condamnat, în ultimii trei ani, prin hotărârea definitivă a unei instanțe

judecătorești, pentru o faptă care a adus atingere eticii profesionale sau pentru comiterea unei greșeli în materie profesională;

d. prezintă informații false sau nu prezintă informațiile solicitate de către autoritatea contractantă, în scopul demonstrării îndeplinirii criteriilor de calificare și selecție;

e. a încălcat obligațiile aplicabile în domeniul mediului, muncii și asigurărilor sociale, în cazul în care autoritatea contractantă demonstrează, prin orice mijloace adecvate, acest fapt;

f. se face vinovat de o abatere profesională, care îi pune la îndoială integritatea, în cazul în care autoritatea contractantă demonstrează, prin orice mijloace adecvate, acest fapt;

g. a încheiat cu alți operatori economici acorduri care vizează denaturarea concurenței, în cazul în care acest fapt se constată printr-o decizie a organului abilitat în acest sens;

h. se află într-o situație de conflict de interese care nu poate fi remediată în mod efectiv prin măsurile prevăzute la art.74 din Legea nr. 131/2015;

i. este inclus în Lista de interdicție a operatorilor economici.

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

11.5. Autoritatea contractantă extrage informația necesară pentru constatarea existenței sau inexistenței circumstanțelor menționate la punctele IPO11.2 și IPO11.3 din bazele de date disponibile ale autorităților publice sau ale părților terțe. Dacă acest lucru nu este posibil, autoritatea contractantă are obligația de a accepta ca fiind suficient și relevant pentru demonstrarea faptului că ofertantul/candidatul nu se încadrează în una dintre situațiile prevăzute menționate la punctele IPO11.2 și IPO11.3 orice document considerat edificator, din acest punct de vedere, în țara de origine sau în țara în care ofertantul este stabilit, cum ar fi certificate, caziere judiciare sau alte documente echivalente emise de autorități competente din țara respectivă.

11.6. În ceea ce privește cazurile menționate la punctul IPO11.3, în conformitate cu legislația internă a statului în care sunt stabiliți ofertanții, aceste solicitări se referă la persoane fizice și persoane juridice, inclusiv, după caz, la directori de companii sau la orice persoană cu putere de reprezentare, de decizie ori de control în ceea ce privește ofertantul/candidatul.

11.7. În cazul în care în țara de origine sau în țara în care este stabilit ofertantul/candidatul nu se emit documente de natura celor prevăzute la punctul IPO11.4 sau respectivele documente nu vizează toate situațiile prevăzute la punctele IPO11.2 și IPO11.3, autoritatea contractantă are obligația de a accepta o declarație pe propria răspundere sau, dacă în țara respectivă nu există prevederi legale referitoare la declarația pe propria răspundere, o declarație autentică dată în fața unui notar, a unei autorități administrative sau judiciare sau a unei asociații profesionale care are competențe în acest sens.

11.8. Orice operator economic aflat în oricare dintre situațiile prevăzute la punctele IPO11.2 și IPO11.3 care atrag excluderea din procedura de atribuire poate furniza dovezi care să arate că măsurile luate de acesta sunt suficiente pentru a-și demonstra în concret credibilitatea prin raportare la motivele de excludere, cu excepția cazului în care operatorul economic a fost exclus prin hotărâre definitivă a unei instanțe de judecată de la participarea la procedurile de achiziții publice.

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

12. Capacitatea de exercitare a activității profesionale

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

13. Capacitatea economică și financiară

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

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

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

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 câștigător îi sînt atribuite mai multe loturi care trebuie executate în același timp.

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

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

13.6. În cazul prevăzut la punctul IPO13.5, ofertantul/candidatul are obligația de a dovedi susținerea de care beneficiază prin prezentarea în formă scrisă a unui angajament ferm al persoanei respective, încheiat în formă autentică, prin care această persoană confirmă faptul că va pune la dispoziția ofertantului/candidatului resursele financiare invocate.

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

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

14. Capacitate tehnică și/sau profesională

14.1. În cazul aplicării unei proceduri pentru atribuirea unui contract de achiziții de bunuri, în scopul verificării capacității tehnice și/sau profesionale a ofertanților, autoritatea contractantă are dreptul de a le solicita acestora, în funcție de specificul, de cantitatea și de complexitatea bunurilor ce urmează să fie furnizate și numai în măsura în care aceste informații sunt relevante pentru îndeplinirea contractului și nu sînt disponibile în bazele de date ale autorităților publice sau ale părților terțe, următoarele:

- a. o listă a principalelor livrări de bunuri similare efectuate în ultimii 3 ani, conținînd valori, perioade de livrare, beneficiari, indiferent dacă aceștia din urmă sunt autorități contractante sau clienți privați. Livrările de bunuri se confirmă prin prezentarea unor certificate/documente emise sau contrasemnate de o autoritate ori de către clientul beneficiar. În cazul în care

beneficiarul este un client privat și, din motive obiective, operatorul economic nu are posibilitatea obținerii unei certificări/confirmări din partea acestuia, demonstrarea livrărilor de bunuri se realizează printr-o declarație a operatorului economic;

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

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

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

e. mostre (în măsura în care necesitatea prezentării este justificată), descrieri și/sau fotografii a căror autenticitate trebuie să poată fi demonstrată în cazul în care autoritatea contractantă solicită acest lucru, dovada experienței specifice în livrarea bunurilor;

f. capacitate minimă de producere sau echipamentele și/sau capacitate minimă profesională

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

14.3. În cazul prevăzut la punctul IPO14.2, ofertantul/candidatul are obligația de a dovedi susținerea de care beneficiază prin prezentarea în formă scrisă a unui angajament ferm al persoanei respective, încheiat în formă autentică, prin care această persoană confirmă faptul că va pune la dispoziția ofertantului/candidatului resursele financiare invocate.

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

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

15. Standarde de asigurare a calității.

15.1. Autoritatea contractantă solicită prezentarea unor certificate, emise de organisme independente, prin care se atestă faptul că operatorul economic respectă anumite standarde de asigurare a calității, aceasta trebuie să se raporteze la sistemele de asigurare a calității, bazate pe seriile de standarde europene relevante, certificate de organisme conforme cu seriile de standarde europene privind certificarea, sau la standarde internaționale pertinente, emise de organisme acreditate.

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

16. Standarde de protecție a mediului.

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

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

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

16.2. În conformitate cu principiul recunoașterii reciproce, autoritatea contractantă are

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

17. Calificarea candidaților în cazul asocierii

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

Secțiunea a-3-a. Pregătirea ofertelor

18. Documentele ce constituie oferta

18.1. Oferta va cuprinde următoarele:

- a) propunerea financiară, care va include, după caz, și garanția pentru ofertă;
- b) propunerea tehnică, precum și documente suport și facultative solicitate de autoritatea contractantă;
- c) Documentul unic de achiziții european;

18.2. Operatorii economici vor pregăti ofertele într-o manieră structurată și securizată, ca răspuns la anunțul de participare publicat de către autoritatea contractantă în SIA „RSAP”, și vor depune ofertele în mod electronic, folosind fluxurile interactive de lucru puse la dispoziție de platformele electronice, cu excepția cazurilor prevăzute la art.32 alin.(7) și (11) din Legea 131/2015.

19. Documente pentru demonstrarea conformității bunurilor

19.1. Pentru a stabili conformitatea bunurilor cu cerințele documentelor de atribuire, ofertantul va depune, ca parte a ofertei sale, dovezi documentare ce atestă faptul că bunurile se conformează condițiilor de livrare, specificațiilor tehnice și standardelor specificate în CAPITOLUL IV.

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

20. Oferte alternative

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

21. Garanția pentru ofertă

21.1. Ofertantul va depune, ca parte a ofertei sale, o Garanție pentru ofertă (**F3.2**), după cum

este specificat în **FDA** punctul 3.2.

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

a) în formă de garanție bancară de la o instituție bancară licențiată, valabilă pentru perioada de valabilitate a ofertei sau altă perioadă prelungită, după caz, în conformitate cu punctul IPO23.2; sau

b) transfer pe contul autorității contractante; sau

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

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

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

a) expirarea termenului de valabilitate a garanției pentru ofertă;

b) încheierea unui contract de achiziții publice și depunerea garanției de bună execuție a contractului, dacă o astfel de garanție este prevăzută în documentația de atribuire;

c) suspendarea procedurii de licitație fără încheierea unui contract de achiziții publice;

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

21.5. Garanția pentru ofertă va fi reținută dacă:

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

b) ofertantul câștigător refuză:

- să depună Garanția de bună execuție conform punctului IPO42;

- să semneze contractul conform punctului IPO43.

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

22. Prețuri

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

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

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

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

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

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

23. Termenul de valabilitate a ofertelor

23.1. Ofertele vor rămâne valabile pe parcursul perioadei specificate în **FDA** punctul 3.8. de la data-limită de depunere a ofertei stabilită de autoritatea contractantă. O ofertă valabilă pentru un

termen mai scurt va fi respinsă de către autoritatea contractantă ca fiind necorespunzătoare.

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

24. Valuta ofertei

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

25. Formatul ofertei

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

Secțiunea a-4-a. Depunerea și deschiderea ofertelor

26. Depunerea ofertelor

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

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

27. Termenul limită de depunere a ofertelor

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

28. Oferte întârziate

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

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

29. Modificarea, substituirea și retragerea ofertelor

29.1. În cazul în care documentația de atribuire nu prevede altfel, ofertantul are dreptul să modifice sau să retragă oferta înainte de expirarea termenului de depunere a ofertelor, fără a pierde dreptul de retragere a garanției pentru ofertă. O astfel de modificare este valabilă dacă a fost efectuată înainte de expirarea termenului de depunere a ofertelor.

30. Deschiderea ofertelor

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

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

Secțiunea a-5-a. Evaluarea și compararea ofertelor

31. Confidențialitate

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

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

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

33. Determinarea conformității ofertelor

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

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

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

33.3. Dacă o ofertă nu este conformă cerințelor din documentele de atribuire, ea va fi respinsă de către autoritatea contractantă.

34. Neconformități, erori și omiteri

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

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

35. Evaluarea ofertelor

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

determina caracterul complet al fiecărui document depus.

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

36. Calificarea ofertantului

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

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

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

37. Descalificarea ofertantului

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

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

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

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

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

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

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

38. Anularea procedurii

38.1. Autoritatea contractantă, din propria inițiativă, anulează procedura de achiziție publică în cazurile prevăzute la art. 67, alin. (1) din Legea nr. 131/2015. Autoritatea contractantă are obligația de a comunica prin SIA „RSAP” sau prin alte mijloace de comunicare în cazul în care

autoritatea contractantă desfășoară proceduri în baza art. 32 alin.(7) și (11) din Legea nr. 131/2015, tuturor participanților la procedura de achiziție publică, în cel mult 3 zile de la data anulării, atât încetarea obligațiilor pe care aceștia și le-au creat prin depunerea de oferte, cât și motivul anulării.

Secțiunea a-2-a. Adjudecarea contractului

39. Criteriul de adjudecare

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

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

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

41. Înștiințarea de adjudecare

41.1. Înainte de expirarea perioadei de valabilitate a ofertei, sistemul SIA „RSAP” va permite autorităților contractante pregătirea anunțului de atribuire și a notificării ofertanților, cărora li s-a atribuit sau nu contractul standardizat.

41.2. Comunicarea prin care se realizează informarea este transmisă prin mijloace electronice la adresele indicate de către ofertanți în ofertele acestora.

41.3. Ofertanții necâștigători vor fi informați cu privire la motivele pentru care ofertele lor nu au fost selectate.

42. Garanția de bună execuție

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

42.2. Refuzul ofertantului câștigător de a depune Garanția de bună execuție sau de a semna contractul va constitui motiv suficient pentru anularea adjudecării și reținerea Garanției pentru ofertă. În acest caz, autoritatea contractantă poate adjudeca contractul următorului ofertant cu oferta cea mai bine clasată, a 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 câștigător Formularul contractului (**F5.1**) completat și toate celelalte documente componente ale contractului.

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

44. Dreptul de contestare

44.1. Orice operator economic care consideră că, în cadrul procedurilor de achiziție,

autoritatea contractantă, prin decizia emisă sau prin procedura de achiziție aplicată cu încălcarea legii, a lezat un drept al său recunoscut de lege, în urma cărui fapt el a suportat sau poate suporta prejudicii, are dreptul să conteste decizia sau procedura aplicată de autoritatea contractantă, în modul stabilit de Legea nr. 131/2015.

44.2. 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 până la 5 zile, sau după caz, 10 zile de la data la care a aflat despre circumstanțele ce au servit drept temei pentru contestație, are dreptul să depună la Agenția Națională pentru Soluționarea Contestațiilor o contestație argumentată a acțiunilor, a deciziei ori a procedurii aplicate de autoritatea contractantă.

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

CAPITOLUL II
FIȘA DE DATE A ACHIZIȚIEI (FDA)

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

Instrucțiunile pentru completarea Fișei de Date a Achiziției sunt oferite cu litere cursive.

1. Dispoziții generale

Nr.	Rubrica	Datele Autorității Contractante/Organizatorului procedurii
1.1.	Autoritatea contractantă / Organizatorul procedurii, IDNO:	Banca Națională a Moldovei, cod fiscal: 79592
1.2.	Obiectul achiziției:	Pachete software aferente securității informaționale
1.3.	Numărul și tipul procedurii de achiziție:	Nr. <u>ocds-b3wdp1-MD-1597044662049</u> Licitație deschisă
1.4.	Tipul obiectului de achiziție:	Bunuri
1.5.	Codul CPV:	48000000-8
1.6.	Sursa alocațiilor bugetare/banilor publici și perioada bugetară:	Buget propriu, pentru anul 2020
1.7.	Administratorul alocațiilor bugetare:	Banca Națională a Moldovei
1.8.	Plăți/mijloace financiare din partea partenerului de dezvoltare:	nu se aplică
1.9.	Denumirea cumpărătorului, IDNO:	Banca Națională a Moldovei, cod fiscal: 79592
1.10.	Destinatarul bunurilor/serviciilor/lucrărilor:	Banca Națională a Moldovei
1.11.	Limba de comunicare:	limba română
1.12.	Locul/Modalitatea de transmitere a clarificărilor referitor la documentația de atribuire:	Prin email la adresa: achizitii.contracte@bnm.md sau prin sistemul electronic SIA „RSAP” M-TENDER
1.13.	Contract de achiziție rezervat atelierelor protejate	Nu se aplică
1.14.	Tipul contractului:	Vânzare-cumpărare (bunuri)
1.15.	Condiții speciale de care depinde îndeplinirea contractului (neobligatoriu):	Nu se aplică

2. Lista bunurilor și specificații tehnice:

Nr. d/o	Cod CPV	Denumire bunuri	Unitate a de măsură	Canti-tatea	Specificarea tehnică deplină solicitată, Standarde de referință
Lotul 1: Soluție de protecție, securitate, patch management și disk encryption pentru locurile de muncă					
1.1	48760000-3	Soluție de protecție, securitate, patch management si disk encryption pentru locurile de	buc.	1	<u>Tip:</u> Subscriere anuală pentru soluția de protecție și securitate, pentru 580 locuri de muncă (PC/laptop/VDI) și 750 căsuțe poștale pentru perioada 12.01.2021-12.01.2022). <u>Cantitate:</u> Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul: - 580 locuri de muncă (PC/laptop, VDI) , 750 căsuțe poștale, - Patch management pentru 200 locuri de muncă,

		muncă		- Disk Encryption management pentru 100 locuri de muncă. Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări „AV-TEST”, „VIRUS BULLETIN’S”, „REAL-WORLD PROTECTION”, „MALWARE PROTECTION”) <u>Caracteristici generale ale produsului:</u> Produsul va conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management: • Protecție stații și servere fizice și virtualizate. • Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android. • Protecție și securitate pentru serverele email Microsoft Exchange. <u>Consola de management:</u> Pachetul de instalare să fie livrat ca o mașină virtuală, care conține toate rolurile sau serviciile necesare. Consola nu va necesita o licență suplimentară pentru sistemul de operare. Imaginea de tip template să poată a fi importa în: 1. VMware vSphere 2. Citrix XenServer 3. Microsoft Hyper-V 4. KVM. Consola de management să fie livrată cu o baza de date inclusă, non-relațională. Soluția trebuie să: • fie scalabilă, astfel ca oricare dintre roluri sau servicii să poată fi instalate separat sau împreună pe aceeași sau mai multe VDI-uri. • asigure următoarele roluri: server cu baza de date, server de comunicație, server de actualizare, server de web. • asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale VMware și Citrix prin task din consola de management. • includă un modul load balancer pentru performanța și redundanță • includă mecanisme de configurare a disponibilității pentru serverul cu baze de date (clustering). <u>Cerințe generale produs:</u> Soluția trebuie să: 1. includă un 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. permite vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi și îmbunătățiri, probleme rezolvate, probleme cunoscute 5. afișeze notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție viruși, actualizări de produs disponibile). 6. permite integrarea cu un server Syslog pentru raportarea evenimentelor antivirus. 7. permite instalarea serviciului de SMNP pentru raportarea statusului mașinilor din cadrul componentei de management. 8. permite crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programat, stocată local, pe un server FTP sau în rețea. <u>Inventarierea rețelei – managementul securității</u> Produsul trebuie să: - se integreze cu domenii Active Directory multiple, VMware vCenter, Citrix Xen și să importe inventarul acestor platforme. - permită descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM. - permită descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery. - ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP. - permită instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale. - permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale. - permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus. - ofere posibilitatea de repornire a mașinilor fizice de la distanță. - ofere informații detaliate despre fiecare task inițiat și afișarea statutului lui. - permită configurarea centralizată a clienților antivirus prin intermediul politicilor. - ofere în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizări, Versiunea produsului, Versiunea de semnături. - permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea. <u>Politici:</u> Produsul trebuie să:
--	--	--	--	--

				- permite configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module - conține 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. - permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directoy. - poate 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). <u>Monitorizare și raportare:</u> Produsul trebuie să: - permită setarea de opțiuni specifice pentru afișarea rapoartelor existente. - dețină un panou central care să afișeze statutul modulelor și rapoartele lor pentru perioadele de timp specificate. - conțină rapoarte care prezinta statusul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate. - trimite rapoarte către un număr nelimitat de adrese de email. - permită vizualizarea rapoartelor curente programate de administrator. - permită exportarea rapoartelor în format .pdf si detaliile ca format .csv. - 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. - ofere interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor. - 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) - 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 carantinarea fișierului, ștergerea sau respingerea e-mail-ului) <u>Carantină:</u> - Produsul trebuie să permită restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă. - Locația, fișierele și administrarea Carantinei trebuie să fie efectuată central din consola de management. <u>Utilizatori:</u> - 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. - Utilizatorii să poată fi importați din Microsoft Active Directory sau creați în consola de management. - Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp. <u>Log-uri:</u> - Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare. <u>Protecție stații și servere fizice și virtualizate – caracteristici minime:</u> Soluția antivirus trebuie să: - permită instalarea personalizată a modulelor, - includă un vaccin anti-ransomware, cu actualizări de la producător, pentru protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și blocarea procesului de criptare. - includă protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate). - 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. - 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. - includă două variante de analiza a sandbox-ului: doar monitorizare sau blocare cu două tipuri de acțiuni de remediere: implicită și de siguranță. Pentru acțiunea implicită: doar raportare, dezinfecție, ștergere și transmitere în carantină. Pentru acțiunea de siguranță: ștergere sau permutare în carantină <u>Cerințe de sistem:</u> -Sisteme de operare pentru stații de lucru: Windows 7 și mai recent, Mac OS X 10.10. și mai recent, Red Hat Enterprise Linux / CentOS 6 și mai recent, Oracle Linux 6.3 și mai recent, Ubuntu 14.04 și mai recent, SUSE Linux Enterprise Server 11 și mai recent, OpenSUSE 42 și mai recent, Fedora 25 și mai recent, Debian 8.0 și mai recent. -Sisteme de operare Windows pentru servere: Windows Server 2008/2008 R2/2012/2012 R2/2016/2019. <u>Administrare și instalare remote:</u> -Pachetele de instalare trebuie să fie configurabile cu modulele necesare: firewall, content control, device control, power user. -Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management. -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. -Produsul trebuie să ofere posibilitatea de a crea pachetele de instalare de tip web installer sau kit full. -Produsul trebuie să permită selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domen. <u>Caracteristici și funcționalități principale ale modului antivirus</u> Produsul trebuie să permită: -stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni: 1. implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune. 2. alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină.
--	--	--	--	--	--

				3. acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune. 4. acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină. -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. -scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de viruși necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă. -scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). -scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP. -configurarea căilor ce urmează a fi scanate la cerere. -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. -setarea priorităților scanărilor programate. -configurarea scanării în cloud sau pe mașina de scanare instalată în rețea și parțial scanarea locală pentru stațiile ce nu au suficiente resurse hardware -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. -setarea a tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazate pe monitorizarea proceselor. -scanarea paginilor web. -setarea a unei parole pentru protecția la dezinstalare. -modul de antiphishing. -protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată. -instalarea clientului pe mașinile virtuale parte a unui pool doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale. <u>Firewall:</u>
--	--	--	--	---

				- sa ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. - modulul să poată fi instalat/dezinstalat la cerere. - să permită definirea de rețele de încredere pentru mașina destinație. <u>Protecția datelor:</u> - Produsul trebuie să permită blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. <u>Controlul conținutului:</u> 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). <u>Controlul aplicațiilor:</u> Pentru administrare și inventariere eficientă produsul trebuie să dețină un modul care va oferi posibilitatea de a: - efectua descoperirea aplicațiilor utilizate pe stațiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe. - regăsi toate procesele descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe. - bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subproces) după: cale fișier: local, CD-ROM, portabil sau rețea, hash , certificat. <u>Controlul dispozitivelor:</u> Produsul trebuie să conțină un modul pentru controlul dispozitivelor care: - poate fi instalat/dezinstalat conform setărilor stabilite. - 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. - permite configurarea de reguli prin care se vor
--	--	--	--	--

					defini permisiunile pentru dispozitivele conectate la mașina client. - permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. <u>Power User:</u> Produsul trebuie să conțină un modul pentru setări specifice – power user care să: - poată fi instalat/dezinstalat în funcție de preferința administratorului. - 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. - permită administratorului soluției să suprascrive din consola setările aplicate de utilizatorii Power User. <u>Actualizare:</u> Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor: - la nivel de stație în mod silențios (fără avertizări). - folosind unul sau mai multe servere de actualizare. - pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare. <u>Protecție și securitate pentru telefoane mobile de tip smartphone:</u> 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: - permită asocierea unui dispozitiv cu un utilizator din Active Directory. - ofere posibilitatea instalării prin trimiterea unui email către utilizator cu detaliile de instalare. - permită activarea dispozitivului mobil în consola de management prin scanarea unui cod QR. - asigure disponibilitatea pachetele de instalare pe Apple App Store si Google Play. - 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). - 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). - întreprindă automat acțiuni în cazul în care un
--	--	--	--	--	---

					dispozitiv nu este conform cu setările dorite: Ignorare; Blocarea accesului; Blocarea dispozitivului; Ștergerea datelor și revenirea la setările din fabrică; Ștergerea dispozitivului din consola. - 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. - ofere posibilitate de a genera mai multe profiluri care vor stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS) dar și unele legate de accesul la anumite pagini de internet. precum: permiterea, blocarea sau programarea pentru anumite zile și intervale orare a accesului la anumite pagini de internet; crearea unor excepții pentru blocarea sau permiterea accesului către anumite pagini de internet. - includă posibilitatea de configurare profilurile acces pagini de internet pentru sistemul de operare iOS cu opțiuni de activare sau dezactivare a: utilizării browser-ului Safari; opțiunii de completare 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: - 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. - asigure scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail. - asigure actualizarea antivirus automat la un interval de maxim 1 ora, precum și la cerere. - includă, pe lângă detecția pe baza de semnături, scanarea euristică comportamentală pentru a proteja sistemul de viruși necunoscuți prin detectarea codurilor. - ofere opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfecție, ștergere, mutare în carantină). - ofere protecție anti-spyware (cu bază de semnături actualizabilă) pentru a preveni furtul de date confidențiale. - 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. - 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. - ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute. - ofere posibilitatea de a defini politici de filtrare antivirus, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori. - 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. - ofere statistici atât referitoare la scanarea antivirus cât și la scanarea antispam. - se integreze în cadrul consolei de management unitar al soluției antivirus în consola centrală unică. <u>Patch management:</u> Soluție pentru managementul actualizării aplicațiilor exploatate* pentru 200 stații de lucru: Bitdefender GravityZone Patch Managemnt sau echivalentul. Soluția trebuie să acopere următoarele funcționalități minime: -Integrarea clientului de patch managemnt cu clientul Antivirus, ca un modul separat. -Administrarea produsului trebuie să fie realizată din aceeași consolă de management ca și soluția de protecție antivirus pentru mediul fizic (stații și servere), mediul virtual (VDI-uri si servere virtuale), căsuțe de email Exchange si dispozitive mobile (Android si iOS). -Abilitatea de a funcționa în mod automat cu următoarele presetări: a. Programarea evaluării pentru patch-ul lipsă b. Programarea instalării automate, în baza categoriei de patch-uri (securitate / non-securitate) c. Posibilitatea de a amâna repornirea, dacă instalarea patch-ului o cere. -Opțiunea de a iniția scanarea, descoperirea și instalarea de patch-uri la cerere. -Posibilitatea de a vedea toate patch-urile care lipsesc din infrastructură și agregarea lor într-un inventar de patch-uri.
--	--	--	--	--	--

				- Vizibilitatea de patch-uri instalate și a celor lipsă pe stațiile de lucru. - Informații despre patch-uri instalate și motivul sau cauza instalării nereușite . - Posibilități de a instala rapid patch-uri lipsă. - Posibilitatea de a stopa instalarea unuia sau a mai multor patch-uri/update-uri. - Notificarea periodică privind statul infrastructurii, patch-uri instalate, patch-uri lipsă - Stocarea locală a patch-urilor primite. <i>*- (7-Zip, Adobe: Acrobat/Bridge/Creative Cloud/Distiller/Dreamweaver/Flash/Photoshop/Reader, Apache, Apache Tomcat, Apple: iCloud/iTunes/Mobile Device Support/QuickTime/Safari/Software Update, WebEx: Meeting Center/Productivity Tools, Citrix: Receiver/Single Sign-On/Delivery Controller/GoToMeeting/Online Plugin/Provisioning Services/Virtual Delivery Agent/XenApp/XenDesktop, FileZilla, Foxit: PhantomPDF/Reader, Gimp, TightVNC, Google: Chrome Browser for enterprise/Drive/Picasa, Greenshot, KeePass, LibreOffice, ImgBurn, Microsoft: .NET/Azure/DirectX/Dynamics/Exchange Server/Exchange System Manager/Forefront/Internet Explorer/Internet Information Server/Lync/Lync Server/Office/Outlook/Power BI Desktop/Report Viewer/Search/Services for Unix/Sharepoint/Skype/Silverlight/System Center Operations Manager/System Center Virtual Machine Manager/SQL Server/Systems Management Server/Virtual Machine/Virtual PC/Virtual Server/Visual Basic/Visual C++/Windows/Windows Defender/WSUS/Windows Mail/Kerberos, Firefox, Thunderbird, Notepad++, GeForce Experience, Opera, Oracle: OpenOffice/VM VirtualBox, Recuva, Prezi Desktop, RealVNC, PuTTY, Java, TeamViewer, PDF-Xchange, UltraVNC, VLC, VMware: Horizon View Client/Player/Tools/Workstation, WinSCP, Wireshark, Xmind)</i> <u>Disk Encryption</u> <i>Soluție pentru managementul criptării discurilor pentru 100 calculatoare portabile: GravityZone Full DiskEncryption sau echivalentul.</i> <i>Soluția trebuie să acopere următoarele funcționalități minime:</i> - Administrarea produsului trebuie să fie realizată din aceeași consolă de management ca și soluția de protecție antivirus pentru mediul fizic (stații și servere), mediul virtual (VDI-uri si servere virtuale), căsuțe de email Exchange si dispozitive mobile
--	--	--	--	---

					(Android si iOS). - Clientul pentru disk encryption nu trebuie să fie ca un modul separat în cadrul clientului Antivirus. - produsul trebuie să folosească mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows si FileVault pentru Mac OSX. - Produsul trebuie să crypteze hard diskurile stațiilor de lucru integral. - Produsul trebuie să impună autentificarea utilizatorului înainte de startarea sistemului de operare (pre-boot authentication). - Produsul trebuie să păstreze cheile de criptare pe același server de management al protecției antivirus, managementul cheilor utilizate să fie efectuat din aceeași consolă comună, inclusiv recuperarea rapidă a cheilor la solicitarea autorizată. - Produsul trebuie să ofere un raport complet asupra stării de criptare a dispozitivelor inclusiv: numele stației, IP-ul stației, sistemul de operare, ID-ul volumului/partiției, numele partiției, starea criptării partiției, tipul partiției: boot, non-boot, mărimea partiției în GB, ID-ul cheii de recuperare. - Produsul trebuie să asigure criptarea pentru Următoarele OS: Windows 7 Enterprise (with TPM); Windows 8.1 Pro/ Enterprise; Windows 10 Pro/ Enterprise; WindowsServer 2008 R2 (withTPM); WindowsServer 2012/2012 R2, WindowsServer 2016, OSX 10.9/ 10.10 / 10.11/ 10.12 Alte cerințe: <u>Perioada de suport și mentinere de la producător:</u> 1. Pentru soluția oferită se solicită a fi 12 luni pentru perioada 12.01.2021-12.01.2022. 2. Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță. <u>Notă:</u> Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă. Termen de livrare: obligatoriu în perioada 01.12.2020 - 25.12.2020, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.
Lotul 2: Menținerea licențelor McAfee					
2.1	72268000-1	Servicii de asigurare a accesului la suport anual Business Support, sau echivalentul, pentru licențe McAfee Total Protection for Data Loss Prevention Software, pentru 400	buc.	1	Tip: Serviciile de asigurare a accesului la suport anual Business Support, sau echivalentul, de la producătorul licențelor McAfee, sunt necesar să fie oferite în baza prelungirii termenului de prestare a serviciilor respective pentru perioada 14.12.2020-13.12.2021 pentru licențele McAfee Total Protection for Data Loss Prevention Software exploatate în cadrul Sistemului Informațional al BNM pentru 400 utilizatori și vor include: - prezentarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau - publicarea informației confirmative pe site-ul producătorului. Cerințe față de serviciile de suport:

		licențe			- Daily product updates (.DATs, engines, etc.) - Product upgrades - Malware alerts with remediation analysis - Malware analysis service - Malware trend podcasts and blogs - Chat, web, and phone support with remote desktop control - 24/7 phone support (normally under 5 minutes to expert), unlimited number of calls to McAfee Technical Support - Automatic diagnostic and remediation tools - Online product test environments. Termen de prestare: obligatoriu în perioada 01.11.2020 - 14.12.2020 inclusiv.
2.2	48219100-7	Subscriere anuală pentru licența McAfee Web Protection, inclusiv 1 an de suport anual Business Support, sau echivalentul, pentru 400 utilizatori	buc.	1	Tip: Subscriere anuale pentru perioada de la 07.11.2020 până la 06.11.2021 pentru licența pentru 400 utilizatori McAfee Web Protection exploatată în cadrul Sistemului Informațional al BNM, cu un an de suport de tipul Business Support inclus, sau echivalentul Cantitate: 1 licență pentru 400 utilizatori. Cerințe față de serviciile de suport: - Daily product updates (.DATs, engines, etc.) - Product upgrades - Malware alerts with remediation analysis - Malware analysis service - Malware trend podcasts and blogs - Chat, web, and phone support with remote desktop control 24/7 phone support (normally under 5 minutes to expert), unlimited number of calls to McAfee Technical Support - Automatic diagnostic and remediation tools - Online product test environments. Termen de livrare: obligatoriu în perioada 01.10.2020 - 07.11.2020 inclusiv.
Lotul 3: Menținerea soluției IBM QRadar					
3.1	72267000-4	Servicii de asigurare a accesului la menținerea anuală a instrumentului i IBM Security QRadar	buc.	1	Tip: Serviciile de asigurare a accesului la suport anual de la producătorul licențelor de tip Annual Software Subscription & Support Renewal 12 Months, sau echivalentul, pentru perioada 01.11.2020 - 31.10.2021, a instrumentului exploatat în cadrul Sistemului Informațional al BNM cu următoarea componență: - IBM Security QRadar SIEM All-in-One Virtual 3190 Install (licență de bază) – 1 buc. IBM Security QRadar Virtual SIEM Event Capacity Increase of 100 EPS Install (pachete adiționale) – 9 buc. Termen de prestare: Confirmarea prestării serviciilor trebuie să fie prezentată obligatoriu în perioada 01.10.2020 - 30.10.2020 inclusiv, și va include: - furnizarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau - publicarea informației confirmative pe site-ul producătorului.
3.2	72267000-4	Servicii de asigurare a accesului la	buc.	1	Tip: Serviciile de asigurare a accesului la suport anual de la producătorul licențelor de tip Annual Software

		menținerea anuală a modului IBM Security QRadar Vulnerability Manager			Subscription & Support Renewal 12 Months, sau echivalentul, a modului IBM Security QRadar Vulnerability Manager, trebuie să fie egalată cu perioada de suport pentru Instrumentul IBM Security QRadar indicat la prima poziție, până la 31.10.2021, cu următoarea componență: • IBM QRadar Software Node Install License - 1 licență pentru consola de roluri de software • IBM Security QRadar Vulnerability Manager Software 60XX Install License – 1 licență pentru scanarea la vulnerabilități a 256 resurse informaționale (assets) și managementul de configurare standard a 50 de resurse Termen de prestare: Confirmarea prestării serviciilor trebuie să fie prezentată obligator în perioada 01.10.2020 - 30.10.2020 inclusiv, și va include: - furnizarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau - publicarea informației confirmative pe site-ul producătorului.
Lotul 4: Soluție integrată pentru gestionarea aplicațiilor și dispozitivelor mobile					
4.1	48730000-4	Soluție integrată pentru gestionarea aplicațiilor și dispozitivelor mobile, cu 12 luni suport standard de la Producător inclus	buc.	1	Tip: Licență pentru soluția integrată pentru gestionarea aplicațiilor și dispozitivelor mobile pentru 50 utilizatori, cu 12 luni suport standard de la Producător inclus, care sa cuprindă tehnologii moderne pentru gestionarea aplicațiilor și dispozitivelor mobile cu un grad de protecție ridicat. Cantitate: Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul asigurarea cu licență pentru 50 utilizatori cu posibilitatea asignării până la 5 dispozitive per utilizator precum și posibilitatea extinderii ulterioare a numărului de licențe. Nota: Ofertantul va veni cu o soluție care va acoperi partea de software necesară pentru întreaga soluție cu respectarea cerințelor specificate mai jos: Cerințe tehnice și specifice: Sistemul propus trebuie să fie o soluție inovatoare, care să asigure următoarele cerințe: 1.Cerințe pentru Securitatea datelor corporative: • Controlul securizat al accesului la datele corporative; • Autentificare bifactorială la datele corporative; • Prevenirea pierderilor de date (DLP); • Posibilitatea de implementare a politicilor de criptare (dispozitiv, SD); • Posibilitatea de securizare și control pentru E-mail și DLP: - Control asupra atașamentelor email; - Control asupra datelor inserate sau copiate; • Posibilitatea de securizare și control al browser-ului mobil; • Posibilitatea de ștergere condiționată a datelor corporative de pe dispozitivele mobile;

				• Posibilitatea de a lucra offline (nu necesită o conexiune permanentă la server pentru identificarea și eliminarea amenințărilor pe dispozitive); • Partajarea datelor corporative de cele personale(BYOD); • Posibilitatea de creare a canalului VPN securizat per aplicație (inclusiv Windows); 2.Cerințe pentru Managementul Aplicațiilor: • Identificarea aplicațiilor mobile instalate și posibilitatea de distribuție a aplicațiilor noi; • Posibilitatea de categorizare a aplicațiilor mobile; • Posibilitatea de creare a listelor admise/interzise de aplicații mobile; • Posibilitatea de creare a restricțiilor pentru rețele wifi • Managementul aplicațiilor mobile (magazine intern de aplicații mobile); • Publicare și livrare centralizată sigură a aplicațiilor mobile; • Containerizarea aplicațiilor mobile; 3. Cerințe pentru Managementul dispozitivelor; • Posibilitatea de încadrare a dispozitivelor mobile personale, în mediul corporativ (BYOD); • Posibilitatea utilizatorilor de auto-înrolare a dispozitivelor mobile (self-service) în sistem; • Posibilitatea de integrare a soluției cu infrastructura existentă a întreprinderii; - Active Directory; - Aplicații interne a companiei (aplicații Web, Mobile); - FileServer; - SIEM; • Managementul conținutului dispozitivului mobil; • Managementul dispozitivelor mobile; • Posibilitatea de creare a modului de lucru KIOSK; • Geo-localizarea dispozitivelor mobile; • Suport pentru o gamă extinsă de platforme: - Windows 10 Desktop; - MacOS; - Android; - iOS; • Sistemul trebuie să ofere funcții avansate de gestionare pentru PC-urile Windows 10 precum: - personalizarea aspectului sistemului; - executarea scripturilor PowerShell (.ps1); - executarea de scripturi pentru modificarea registrului (.reg); - setarea BitLocker pentru criptarea discului; - gestionarea drepturilor utilizatorului; - setarea accesului la funcțiile Windows (meniul de setări); - instalarea oricărui GPO prin registru; - gestionarea sistemului de fișiere; - instalarea de drivere; - instalarea aplicațiilor LOB;
--	--	--	--	--

				- instalarea pachetelor software; - dezinstalarea software-ului preinstalat; - gestionarea imprimantei, etc.; 4. Cerințe pentru Serverul de administrare: • Instalarea componentelor serverului soluției nu trebuie să necesite preinstalarea unui sistem de operare separat și a unei baze de date separate, precum și a licențelor lor separate • Posibilitatea de a instala componente suplimentare de server: - pentru a asigura funcționarea sistemului cu disponibilitate ridicată (high availability) - posibilitatea utilizării în scopuri de testare înainte de a adăuga orice funcționalitate în mediul de lucru • Soluția trebuie să asigure extinderea cu ușurință a dispozitivelor gestionate • Posibilitatea de update a soluției direct din consola de administrare, fără implicarea directă a producătorului • Android Enterprise suport pentru dispozitivele BYOD 5. Certificări conform standardelor internaționale: • FIPS 140-2; • ISO/IEC 27001:2013; • Common Criteria Certification; Cerința de certificare poate fi demonstrată prin prezentarea copiei certificatului, sau referință pe site-ul producătorului. Alte cerințe obligatorii: <u>Perioada de suport și mentinere de la producător:</u> 3. Pentru soluția oferită se solicită a fi pentru o perioadă de 12 luni din data acceptanței soluției. 4. Producătorul trebuie să ofere: - suport 24/24, prin e-mail sau conectare de la distanță, - asigurarea accesului la update-uri și Baza de cunoștințe (Knowledge Base + Product Updates) <u>Notă:</u> Lucrările de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției precum și transferul de cunoștințe trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă. Termen de livrare: 30 de zile lucrătoare din data intrării în vigoare a contractului care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.
--	--	--	--	---

3. Pregătirea ofertelor

3.1.	Oferte alternative:	nu se acceptă
3.2.	Garanția pentru ofertă:	<u>Forma garanției:</u> a) Garanția pentru ofertă prin transfer la contul autorității contractante, conform următoarelor date bancare:

		<i>Beneficiarul plății: Banca Națională a Moldovei</i> <i>Denumirea Băncii: Banca Națională a Moldovei</i> <i>Codul fiscal: 79592</i> <i>IBAN: MD12NB0000000000004914852</i> <i>Contul bancar: NBMDMD2X</i> <i>cu nota "Pentru garanția pentru ofertă la procedura de achiziție prin LD"</i> sau <i>b) Oferta va fi însoțită de o Garanție pentru ofertă (emisă de o bancă) conform formularului F3.2 din secțiunea a 3-a – Formulare pentru depunerea ofertei</i>
3.3.	Garanția pentru ofertă va fi în valoare de:	<i>1 % din valoarea ofertei fără TVA.</i>
3.4.	Ediția aplicabilă a Incoterms și termenii comerciali acceptați vor fi:	<i>Nu se aplică</i>
3.5.	Termenul de livrare/prestare:	<i>Toate bunurile/serviciile vor fi livrate și/sau prestate de către Vanzător/Prestator la sediul Cumpărătorului/Beneficiarului în termenele indicate pe fiecare lot în parte. Vanzătorul/Prestatorul va asigura livrarea bunurilor și/sau prestarea serviciilor în corespundere cu toate cerințele înaintate.</i>
3.6.	Locul livrării/prestării bunurilor/serviciilor:	<i>bd. Grigore Vieru 1, mun. Chișinău, MD-2005, Republica Moldova</i>
3.7.	Metoda și condițiile de plată vor fi:	<i>Achitarea Bunurilor/Serviciilor de către Cumpărător/Beneficiar se va efectua: Integral după livrarea bunurilor și/sau prestarea serviciilor, în decurs de 15 zile lucrătoare, în baza actului de primire-predare a bunurilor și/sau a serviciilor semnat de reprezentanții ambelor părți și a facturii fiscale.</i>
3.8.	Perioada valabilității ofertei va fi de:	<i>60 zile calendaristice</i>
3.9.	Ofertele în valută străină:	<i>Se acceptă</i>

4. Depunerea și deschiderea ofertelor

4.1.	Locul/Modalitatea de depunere a ofertelor, este	<i>Ofertele vor fi depuse electronic prin sistemul SIA „RSAP” M-Tender</i>
4.2.	Termenul limită de depunere a ofertelor este	<i>Data-limită pentru depunerea ofertelor este: 07.09.2020</i> <i>Data, Ora: 07.09.2020, ora 14:00</i>
4.3.	Persoanele autorizate să asiste la deschiderea ofertelor (cu excepția cazului când ofertele au fost depuse prin SIA „RSAP”)	<i>Deschiderea ofertelor are loc prin intermediul sistemului electronic SIA „RSAP” M-TENDER</i>

5. Evaluarea și compararea ofertelor

5.1.	Prețurile ofertelor depuse în diferite valute vor fi convertite în:	<i>Lei MD</i>
	Sursa ratei de schimb în scopul convertirii:	<i>Cursul oficial stabilit de Banca Națională a Moldovei http://www.bnm.md/en/content/official-exchange-rates</i>
	Data pentru rata de schimb aplicabilă va fi:	<i>Data deschiderii ofertelor</i>
5.2.	Modalitatea de efectuare a evaluării:	<i>Evaluarea va fi efectuată pe fiecare lot separat, cu corespunderea cerințelor față de ofertant și corespunderea tuturor cerințelor tehnice minime obligatorii privind obiectul achiziției.</i>
5.3.	Factorii de evaluare vor fi următorii:	<i>Nu se aplică</i>

6. Adjudecarea contractului

6.1.	Criteriul de evaluare aplicat pentru adjudecarea contractului va fi:	<i>Prețul cel mai scăzut, fără TVA.</i>
6.2.	Suma Garanției de bună execuție (se stabilește procentual din prețul contractului adjudecat):	<i>5 %</i>
6.3.	Garanția de bună execuție a contractului:	<i>Forma garanției de bună execuție:</i> <i>a) Garanția de bună execuție prin transfer la contul autorității contractante, conform următoarelor date bancare:</i> <i>Beneficiarul plății: Banca Națională a Moldovei</i> <i>Denumirea Băncii: Banca Națională a Moldovei</i> <i>Codul fiscal: 79592</i> <i>IBAN: MD65NB0000000000004914771</i> <i>Contul bancar: NBMDMD2X</i> <i>cu nota "Pentru garanția de bună executare a contractului la procedura de achiziție prin LD"</i> sau <i>b) Garanția de bună execuție emisă de o bancă conform formularului F3.3.</i>
6.4.	Forma de organizare juridică pe care trebuie să o ia asocieria grupului de operatori economici cărora li s-a atribuit contractul	<i>Nu se cere</i>
6.5.	Numărul maxim de zile pentru semnarea și prezentarea contractului către autoritatea contractantă:	<i>10 zile calendaristice</i>

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

Conducătorul grupului de lucru:

Aureliu CINCILEI (*semnat electronic*)

CAPITOLUL III
FORMULARE PENTRU DEPUNEREA OFERTEI

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

Formular	Denumirea
F3.1	Formularul ofertei
F3.2	Garanția pentru ofertă
F3.3	Garanția de bună execuție
F3.4	Chestionar pentru Prestator / Furnizor
F3.5	Declarație privind lista principalelor livrări de bunuri similare în ultimii 3 ani

Formularul ofertei (F3.1)

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

Data depunerii ofertei: “___” _____ 20__

Procedura de achiziție Nr.: _____

Anunț de participare Nr.: _____

Către: _____
[numele deplin al autorității contractante]

_____ declară că:
[denumirea ofertantului]

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

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

b) _____ se angajează să furnizeze/
[denumirea ofertantului]
presteze, în conformitate cu documentele de atribuire și condițiile stipulate în specificațiile tehnice și preț, următoarele bunuri

[introduceți o descriere succintă a bunurilor]

c) Suma totală a ofertei fără TVA constituie:

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

d) Suma totală a ofertei cu TVA constituie:

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

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

f) În cazul acceptării prezentei oferte,
_____ se
[denumirea ofertantului]

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

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

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

Semnat: _____
[semnătura persoanei autorizate pentru semnarea ofertei]

Nume: _____

În calitate de: _____
[funcția oficială a persoanei ce semnează formularul ofertei]

Ofertantul: _____

Adresa: _____

Data: “___” _____ 20__

Garanția pentru oferta (F3.2)

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

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

Beneficiar: _____

_____ [numele și adresa autorității contractante]

Data: “___” _____ 20__

GARANȚIE DE OFERTĂ Nr. _____

_____ a fost informată că
_____ [denumirea băncii]

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

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

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

La cererea Ofertantului, noi, _____, prin prezenta,
_____ [denumirea băncii]
ne angajăm în mod irevocabil să vă plătim orice sumă sau sume ce nu depășesc în
total suma de:

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

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

a) și-a retras oferta în timpul perioadei valabilității ofertei sau a modificat oferta după expirarea termenului-limită de depunere a ofertelor; sau

b) fiind anunțat de către autoritatea contractantă, în perioada de valabilitate a ofertei, despre adjudecarea contractului: (i) eșuează sau refuză să semneze formularul contractului;; sau (ii) eșuează sau refuză să prezinte garanția de bună execuție, dacă se cere conform condițiilor licitației, ori nu a executat vreo condiție specificată în documentele de atribuire, înainte de semnarea contractului de achiziție.

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

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

_____ [semnătura autorizată a băncii]

Garanție de bună execuție (F3.3)

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

Data: “___” _____ 20__

Licitația Nr.: _____

Oficiul Băncii: _____

[introduceți numele complet al garantului]

Beneficiar: _____

[introduceți numele complet al autorității contractante]

GARANȚIA DE BUNĂ EXECUȚIE

Nr. _____

Noi, *[introduceți numele legal și adresa băncii]*, am fost informați că firmei *[introduceți numele deplin al Prestatorului]* (numit în continuare “Prestator”) i-a fost adjudecat Contractul de achiziție publică de prestare _____ *[obiectul achiziției, descrieți serviciile]* conform invitației la licitația nr. _____ din _____ 201_ *[numărul și data licitației]* (numit în continuare “Contract”).

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

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

Această Garanție va expira nu mai târziu de *[introduceți numărul]* de la data de *[introduceți luna][introduceți anul]*,¹ și orice cerere de plată ce ține de aceasta trebuie recepționată de către noi la oficiu pînă la această dată inclusiv.

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

[semnăturile reprezentanților autorizați ai băncii și ai Prestatorului]

CHESTIONAR PENTRU PRESATOR/FURNIZOR (F3.4)

1. Date despre Prestator/Furnizor (persoană juridică/persoană fizică)

- 1.1 Denumirea completă/ Nume, prenume _____
- 1.2 Forma de organizare juridică/ - _____
- 1.3 Codul fiscal/IDNO _____
- 1.4 Numărul și data înregistrării de stat/expus politic (Da/Nu) _____
- 1.5 Sediul și adresa juridică/adresa de domiciliu _____
- 1.6 Numărul de telefon, fax, email _____
- 1.7 Persoana împuternicită să deschidă și să gestioneze contul
 - 1.7.1 Numele, prenumele _____
 - 1.7.2 Data și locul nașterii, IDNO _____
 - 1.7.3 Adresa de domiciliu _____
 - 1.7.4 Funcția deținută _____
 - 1.7.5 Telefon, fax, e-mail _____
 - 1.7.6 Expus politic (Da/Nu) _____

2. Informație privind natura relației de afaceri cu BNM

2.1 Domeniul de activitate

2.2 Scopul și motivul inițierii relației de afaceri / tranzacții ocazionale

2.3 Activități preconizate

3. Declarația privind beneficiarul efectiv

3.1 Beneficiarul efectiv este următoarea persoană:

3.2 Date despre beneficiarul efectiv :

- 3.2.1 Numele, prenumele _____
- 3.2.2 Data și locul nașterii, IDNO _____
- 3.2.3 Adresa de domiciliu _____
- 3.2.4 Funcția deținută _____
- 3.2.5 Telefon, fax, email _____
- 3.2.6 Expus politic (Da/Nu) _____

Data ____/____/____

Semnătura prestator/furnizor

_____ L.S

beneficiar efectiv – persoană fizică ce deține sau controlează în ultimă instanță o persoană fizică sau juridică ori beneficiar al unei societăți de investiții sau administrator al societății de investiții, ori persoană în al cărei nume se desfășoară o activitate sau se realizează o tranzacție și/sau care deține, direct sau indirect, dreptul de proprietate sau controlul asupra a cel puțin 25% din acțiuni sau din dreptul de vot al persoanei juridice ori asupra bunurilor aflate în administrare fiduciară;

Parlamentul Republicii Moldova 308/22.12.2017 Lege cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului *Monitorul Oficial al R. Moldova*, 58-66/133, 23.02.2018

¹ Conform Hotărârii Guvernului nr.693 din 04 octombrie 1991 Institutul Bancar Român are în calitate de fondatori Banca Națională a României și Asociația Română a Băncilor, respectiv, nu există un beneficiar efectiv în sensul definiției date de Legea RM nr.308 din 22.12.2017

**DECLARAȚIE PRIVIND LISTA PRINCIPALELOR LIVRĂRI
DE BUNURI SIMILARE ÎN ULTIMII 3 ANI (F3.5)**

Operator economic

(denumirea/numele)

Subsemnatul, reprezentant împuternicit al <denumirea/numele și sediul/adresa candidatului/Ofertantului>, declar pe propria răspundere, sub sancțiunile aplicate faptei de fals în acte publice, că datele prezentate în tabelul anexat sunt reale.

Subsemnatul declar că informațiile furnizate sunt complete și corecte în fiecare detaliu și înțeleg că Beneficiarul are dreptul de a solicita, în scopul verificării și confirmării declarațiilor, situațiilor și documentelor care însoțesc oferta, orice informații suplimentare în scopul verificării datelor din prezenta declarație.

Subsemnatul autorizez prin prezenta orice instituție, societate comercială, bancă, alte persoane juridice să furnizeze informații reprezentanților autorizați ai Băncii Naționale a Moldovei, cu privire la orice aspect tehnic și financiar în legătura cu activitatea noastră.

Lista principalelor livrări de bunuri similare:

Nr crt	Numărul și Obiectul contractu lui / Tipul bunurilor livrate	Scopul livrării bunurilor	Calitatea în care a participat la îndeplinire a contractulu i (*)	Procent îndeplin it de către Ofertant (%)	Denumirea/ numele, sediul/adresa beneficiarului /clientului/ pagina web	Perioada de derulare a contractul ui (**)	Prețul total al contract ului în MDL
0	1	2	3	4	5	6	7
1							
2							
3							
4	TOTAL			-			

Data completării :[ZZ.LL.AAAA]

Operator economic,

.....

(nume și semnătura autorizată)

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

**) Se vor preciza data de începere și data inițială (prelungită) de finalizare a contractului.

CAPITOLUL IV
SPECIFICAȚII TEHNICE ȘI DE PREȚ

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

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

Specificații tehnice (F4.1)

În cazul unei discrepanțe sau al unui conflict cu cerințele din secțiunea 2. Fișa de date a achiziției (FDA), prevederile din FDA vor prevala asupra prevederilor de mai jos.

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

Numărul procedurii de achiziție nr. <u>ocds-b3wdp1-MD-1597044662049</u> din 07.09.2020
Denumirea procedurii de achiziție: <i>Pachete software aferente securității informaționale</i>

Cod CPV	Denumirea bunurilor	Modelul articolului	Țara de origine	Produsul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7	8
Lotul 1: Soluție de protecție, securitate, patch management și disk encryption pentru locurile de muncă							
48760 000-3	Soluție de protecție, securitate, patch management și disk encryption pentru locurile de muncă				<u>Tip:</u> Subscriere anuală pentru soluția de protecție și securitate, pentru 580 locuri de muncă (PC/laptop/VDI) și 750 căsuțe poștale pentru perioada 12.01.2021-12.01.2022). <u>Cantitate:</u> Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul: - 580 locuri de muncă (PC/laptop, VDI) , 750 căsuțe poștale, - Patch management pentru 200 locuri de muncă, - Disk Encryption management pentru 100 locuri de muncă. Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări „AV-TEST”, „VIRUS BULLETIN’S”, „REAL-WORLD PROTECTION”, „MALWARE PROTECTION”) <u>Caracteristici generale ale produsului:</u> Produsul va conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management: • Protecție stații și servere fizice și virtualizate. • Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android.		Nu se aplică

					• Protecție și securitate pentru serverele email Microsoft Exchange. <u>Consola de management:</u> Pachetul de instalare să fie livrat ca o mașină virtuală, care conține toate rolurile sau serviciile necesare. Consola nu va necesita o licență suplimentară pentru sistemul de operare. Imaginea de tip template să poată a fi importa în: 1. VMware vSphere 2. Citrix XenServer 3. Microsoft Hyper-V 4. KVM. Consola de management să fie livrată cu o baza de date inclusă, non-relațională. Soluția trebuie să: • fie scalabilă, astfel ca oricare dintre roluri sau servicii să poată fi instalate separat sau împreună pe aceeași sau mai multe VDI-uri. • asigure următoarele roluri: server cu baza de date, server de comunicație, server de actualizare, server de web. • asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale VMware și Citrix prin task din consola de management. • includă un modul load balancer pentru performanța și redundanță • includă mecanisme de configurare a disponibilității pentru serverul cu baze de date (clustering). <u>Cerințe generale produs:</u> Soluția trebuie să: - includă un unul sau mai multe module de update server prin care să asigure actualizarea componentelor și a semnăturilor. - permită activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management. - transmită alerte de ne funcționalitate, cu 30 de minute		
--	--	--	--	--	---	--	--

					înainte de actualizare. - permită vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi și îmbunătățiri, probleme rezolvate, probleme cunoscute - afișeze notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție viruși, actualizări de produs disponibile). - permită integrarea cu un server Syslog pentru raportarea evenimentelor antivirus. - permită instalarea serviciului de SMNP pentru raportarea statusului mașinilor din cadrul componentei de management. - permită crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programat, stocată local, pe un server FTP sau în rețea. <u>Inventarierea rețelei – managementul securității</u> Produsul trebuie să: - se integreze cu domenii Active Directory multiple, VMware vCenter, Citrix Xen și să importe inventarul acestor platforme. - permită descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM. - permită descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery. - ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP. - permită instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale. - permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale. - permită lansarea de task-uri de scanare, actualizare, instalare, deinstalare la distanță pentru clientul antivirus.		
--	--	--	--	--	---	--	--

					- ofere posibilitatea de repornire a mașinilor fizice de la distanță. - ofere informații detaliate despre fiecare task inițiat și afișarea statutului lui. - permită configurarea centralizată a clienților antivirus prin intermediul politicilor. - 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. - permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea. <u>Politici:</u> Produsul trebuie să: - permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module - 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. - permită aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directory. - 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 acces la rețea cu infrastructura de management, Tipul rețelei (lan, wireless). <u>Monitorizare și raportare:</u> Produsul trebuie să: - permită setarea de opțiuni specifice pentru afișarea rapoartelor existente. - dețină un panou central care să afișeze statutul modulelor și		
--	--	--	--	--	---	--	--

					<i>rapoartele lor pentru perioadele de timp specificate.</i> - <i>conțină rapoarte care prezintă statusul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.</i> - <i>trimită rapoarte către un număr nelimitat de adrese de email.</i> - <i>permite vizualizarea rapoartelor curente programate de administrator.</i> - <i>permite exportarea rapoartelor în format .pdf și detaliile ca format .csv.</i> - <i>include un generator de rapoarte care să ofere posibilitatea de a investiga o problemă de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal, evenimente Exchange.</i> - <i>ofere interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor.</i> - <i>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)</i> - <i>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 carantinarea fișierului, ștergerea sau respingerea e-mail-ului)</i> <u>Carantină:</u> - <i>Produsul trebuie să permită restaurarea fișierelor din</i>		
--	--	--	--	--	---	--	--

					carantină în locația originală sau într-o cale configurabilă. - Locația, fișierele și administrarea Carantinei trebuie să fie efectuată central din consola de management. <u>Utilizatori:</u> - 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. - Utilizatorii să poată fi importați din Microsoft Active Directory sau creați în consola de management. - Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp. <u>Log-uri:</u> - Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare. <u>Protecție stații și servere fizice și virtualizate – caracteristici minime:</u> Soluția antivirus trebuie să: - permită instalarea personalizată a modulelor, - includă un vaccin anti-ransomware, cu actualizări de la producător, pentru protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și blocarea procesului de criptare. - includă protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate). - 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. - 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. - includă două variante de analiza a sandbox-ului: doar monitorizare sau blocare cu două tipuri de acțiuni de remediere: implicită și de siguranță. Pentru acțiunea implicită: doar raportare, dezinfectie, ștergere și transmitere în carantină. Pentru acțiunea de siguranță: ștergere sau permutare în carantină <u>Cerințe de sistem:</u> -Sisteme de operare pentru stații de lucru: Windows 7 și mai recent, Mac OS X 10.10. și mai recent, Red Hat Enterprise Linux / CentOS 6 și mai recent, Oracle Linux 6.3 și mai recent, Ubuntu 14.04 și mai recent, SUSE Linux Enterprise Server 11 și mai recent, OpenSUSE 42 și mai recent, Fedora 25 și mai recent, Debian 8.0 și mai recent. -Sisteme de operare Windows pentru servere: Windows Server 2008/2008 R2/2012/2012 R2/2016/2019. <u>Administrare și instalare remote:</u> -Pachetele de instalare trebuie să fie configurabile cu modulele necesare: firewall, content control, device control, power user. -Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management. -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. -Produsul trebuie să ofere posibilitatea de a crea pachetele de instalare de tip web installer sau kit full. -Produsul trebuie să permită selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în		
--	--	--	--	--	---	--	--

					domen. <u>Caracteristici și funcționalități principale ale modulului antivirus</u> Produsul trebuie să permită: -stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni: 1. implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune. 2. alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină. 3. acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune. 4. acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină. -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. -scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de viruși necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă. -scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). -scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP. -configurarea căilor ce urmează a fi scanate la cerere. -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.		
--	--	--	--	--	---	--	--

				-setarea priorităților scanărilor programate. -configurarea scanării în cloud sau pe mașina de scanare instalată în rețea și parțial scanarea locală pentru stațiile ce nu au suficiente resurse hardware -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. -setarea a tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazate pe monitorizarea proceselor. -scanarea paginilor web. -setarea a unei parole pentru protecția la dezinstalare. -modul de antiphishing. -protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată. -instalarea clientului pe mașinile virtuale parte a unui pool doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale. <u>Firewall:</u> - sa ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. - modulul să poată fi instalat/dezinstalat la cerere. - să permită definirea de rețele de încredere pentru mașina destinație. <u>Protecția datelor:</u> - Produsul trebuie să permită blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. <u>Controlul conținutului:</u> 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). <u>Controlul aplicațiilor:</u> Pentru administrare și inventariere eficientă produsul trebuie să dețină un modul care va oferi posibilitatea de a: - efectua descoperirea aplicațiilor utilizate pe stațiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe. - regăsi toate procesele descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe. - bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subproces) după: cale fișier: local, CD-ROM, portabil sau rețea, hash , certificat. <u>Controlul dispozitivelor:</u> Produsul trebuie să conțină un modul pentru controlul dispozitivelor care: - poate fi instalat/dezinstalat conform setărilor stabilite. - 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. - permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client. - permite configurarea de excluderi pentru diferite tipuri de		
--	--	--	--	--	--	--	--

					dispozitive pentru care s-au configurat reguli. <u>Power User:</u> Produsul trebuie să conțină un modul pentru setări specifice – power user care să: - poată fi instalat/dezinstalat în funcție de preferința administratorului. - 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. - permită administratorului soluției să suprascrive din consola setările aplicate de utilizatorii Power User. <u>Actualizare:</u> Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor: - la nivel de stație în mod silențios (fără avertizări). - folosind unul sau mai multe servere de actualizare. - pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare. <u>Protecție și securitate pentru telefoane mobile de tip smartphone:</u> 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: - permită asocierea unui dispozitiv cu un utilizator din Active Directory. - ofere posibilitatea instalării prin trimiterea unui email către utilizator cu detaliile de instalare. - permită activarea dispozitivului mobil în consola de management prin scanarea unui cod QR. - asigure disponibilitatea pachetele de instalare pe Apple App Store si Google Play. - 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). - 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). - 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. - 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. - 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. - 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>		
--	--	--	--	--	--	--	--

					<i>Soluția de protecție a serverelor de Exchange trebuie să:</i> - 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. - asigure scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail. - asigure actualizarea antivirus automat la un interval de maxim 1 ora, precum și la cerere. - includă, pe lângă detecția pe baza de semnături, scanarea euristică comportamentală pentru a proteja sistemul de viruși necunoscuți prin detectarea codurilor. - ofere opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, ștergere, mutare în carantină). - ofere protecție anti-spyware (cu bază de semnături actualizabilă) pentru a preveni furtul de date confidențiale. - ofere protecție antispam (cu o bază de semnături actualizabilă. Modulul antispam va trebui să includă un filtru URL cu o bază de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice. - 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. - ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute. - ofere posibilitatea de a defini politici de filtrare antivirus, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori. - 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. - ofere statistici atât referitoare la scanarea antivirus cât și la scanarea antispam. - se integreze în cadrul consolei de management unitar al soluției antivirus în consola centrală unică. <u>Patch management:</u> Soluție pentru managementul actualizării aplicațiilor exploatate* pentru 200 stații de lucru: Bitdefender GravityZone Patch Managemnt sau echivalentul. Soluția trebuie să acopere următoarele funcționalități minime: - Integrarea clientului de patch management cu clientul Antivirus, ca un modul separat. - Administrarea produsului trebuie să fie realizată din aceeași consolă de management ca și soluția de protecție antivirus pentru mediul fizic (stații și servere), mediul virtual (VDI-uri și servere virtuale), căsuțe de email Exchange și dispozitive mobile (Android și iOS). - Abilitatea de a funcționa în mod automat cu următoarele presetări: d. Programarea evaluării pentru patch-ul lipsă e. Programarea instalării automate, în baza categoriei de patch-uri (securitate / non-securitate) f. Posibilitatea de a amâna repornirea, dacă instalarea patch-ului o cere. - Opțiunea de a iniția scanarea, descoperirea și instalarea de patch-uri la cerere. - Posibilitatea de a vedea toate patch-urile care lipsesc din infrastructură și agregarea lor într-un inventar de patch-uri. - Vizibilitatea de patch-uri instalate și a celor lipsă pe stațiile de lucru. - Informații despre patch-uri instalate și motivul sau cauza instalării nereușite . - Posibilități de a instala rapid patch-uri lipsă.		
--	--	--	--	--	---	--	--

					-Posibilitatea de a stopa instalarea unuia sau a mai multor patch-uri/update-uri. -Notificarea periodică privind statul infrastructurii, patch-uri instalate, patch-uri lipsă -Stocarea locală a patch-urilor primite. <i>*- (7-Zip, Adobe: Acrobat/Bridge/Creative Cloud/Distiller/Dreamweaver/Flash/Photoshop/Reader, Apache, Apache Tomcat, Apple: iCloud/iTunes/Mobile Device Support/QuickTime/Safari/Software Update, WebEx: Meeting Center/Productivity Tools, Citrix\$ Receiver/Single Sign-On/Delivery Controller/GoToMeeting/Online Plugin/Provisioning Services/Virtual Delivery Agent/XenApp/XenDesktop, FileZilla, Foxit: PhantomPDF/Reader, Gimp, TightVNC, Google: Chrome Browser for enterprise/Drive/Picasa, Greenshot, KeePass, LibreOffice, ImgBurn, Microsoft: .NET/Azure/DirectX/Dynamics/Exchange Server/Exchange System Manager/Forefront/Internet Explorer/Internet Information Server/Lync/Lync Server/Office/Outlook/Power BI Desktop/Report Viewer/Search/Services for Unix/Sharepoint/Skype/Silverlight/System Center Operations Manager/System Center Virtual Machine Manager/SQL Server/Systems Management Server/Virtual Machine/Virtual PC/Virtual Server/Visual Basic/Visual C++/Windows/Windows Defender/WSUS/Windows Mail/Kerberos, Firefox, Thunderbird, Notepad++, GeForce Experience, Opera, Oracle: OpenOffice/VM VirtualBox, Recuva, Prezi Desktop, RealVNC, PuTTY, Java, TeamViewer, PDF-Xchange, UltraVNC, VLC, VMware: Horizon View Client/Player/Tools/Workstation, WinSCP, Wireshark, Xmind)</i> <u>Disk Encryption</u> Soluție pentru managementul criptării discurilor pentru 100 calculatoare portabile: GravityZone Full DiskEncryption sau		
--	--	--	--	--	---	--	--

					echivalentul. Soluția trebuie să acopere următoarele funcționalități minime: - Administrarea produsului trebuie să fie realizată din aceeași consolă de management ca și soluția de protecție antivirus pentru mediul fizic (stații și servere), mediul virtual (VDI-uri și servere virtuale), căsuțe de email Exchange și dispozitive mobile (Android și iOS). - Clientul pentru disk encryption nu trebuie să fie ca un modul separat în cadrul clientului Antivirus. - produsul trebuie să folosească mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows și FileVault pentru Mac OSX. - Produsul trebuie să crypteze hard diskurile stațiilor de lucru integral. - Produsul trebuie să impună autentificarea utilizatorului înainte de startarea sistemului de operare (pre-boot authentication). - Produsul trebuie să păstreze cheile de criptare pe același server de management al protecției antivirus, managementul cheilor utilizate să fie efectuat din aceeași consolă comună, inclusiv recuperarea rapidă a cheilor la solicitarea autorizată. - Produsul trebuie să ofere un raport complet asupra stării de criptare a dispozitivelor inclusiv: numele stației, IP-ul stației, sistemul de operare, ID-ul volumului/partiției, numele partiției, starea criptării partiției, tipul partiției: boot, non-boot, mărimea partiției în GB, ID-ul cheii de recuperare. - Produsul trebuie să asigure criptarea pentru Următoarele OS: Windows 7 Enterprise (with TPM); Windows 8.1 Pro/ Enterprise; Windows 10 Pro/ Enterprise; WindowsServer 2008 R2 (withTPM); WindowsServer 2012/2012 R2, WindowsServer 2016, OSX 10.9/ 10.10 / 10.11/ 10.12 Alte cerințe: <u>Perioada de suport și mentinere de la producător:</u>		
--	--	--	--	--	---	--	--

					1.Pentru soluția ofertată se solicită a fi 12 luni pentru perioada 12.01.2021-12.01.2022. 2.Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță. <u>Notă:</u> Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă. Termen de livrare: obligatoriu în perioada 01.12.2020 - 25.12.2020, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției		
Lotul 2: Menținerea licențelor McAfee							
72268 000-1	Servicii de asigurare a accesului la suport anual Business Support, sau echivalentul, pentru licențe McAfee Total Protection for Data Loss Prevention Software, pentru 400 licențe				Tip: Serviciile de asigurare a accesului la suport anual Business Support, sau echivalentul, de la producătorul licențelor McAfee, sunt necesar să fie oferite în baza prelungirii termenului de prestare a serviciilor respective pentru perioada 14.12.2020-13.12.2021 pentru licențele McAfee Total Protection for Data Loss Prevention Software exploatate în cadrul Sistemului Informațional al BNM pentru 400 utilizatori și vor include: - prezentarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau - publicarea informației confirmative pe site-ul producătorului. Cerințe față de serviciile de suport: - Daily product updates (.DATs, engines, etc.) - Product upgrades - Malware alerts with remediation analysis - Malware analysis service - Malware trend podcasts and blogs - Chat, web, and phone support with remote desktop control - 24/7 phone support (normally under 5 minutes to expert), unlimited number of calls to McAfee Technical Support - Automatic diagnostic and remediation tools - Online product test environments. Termen de prestare: obligatoriu în perioada 01.11.2020 - 14.12.2020		Nu se aplică
482191 00-7	Subscriere anuală pentru				Tip: Subscriere anuale pentru perioada de la 07.11.2020 până la 06.11.2021 pentru licența pentru 400 utilizatori McAfee Web		

	licența McAfee Web Protection, inclusiv 1 an de suport anual Business Support, sau echivalentul, pentru 400 utilizatori				<i>Protection exploatată în cadrul Sistemului Informațional al BNM, cu un an de suport de tipul Business Support inclus, sau echivalentul</i> Cantitate: 1 licență pentru 400 utilizatori. Cerințe față de serviciile de suport: <i>Daily product updates (.DATs, engines, etc.)</i> <i>Product upgrades</i> <i>Malware alerts with remediation analysis</i> <i>Malware analysis service</i> <i>Malware trend podcasts and blogs</i> <i>Chat, web, and phone support with remote desktop control</i> <i>24/7 phone support (normally under 5 minutes to expert), unlimited number of calls to McAfee Technical Support</i> <i>Automatic diagnostic and remediation tools</i> <i>Online product test environments.</i> Termen de livrare: obligator în perioada 01.10.2020 - 07.11.2020 inclusiv.		
Lotul 3: Menținerea soluției IBM Qradar							
72267 000-4	Servicii de asigurare a accesului la menținerea anuală a instrumentului IBM Security Qradar				Tip: Serviciile de asigurare a accesului la suport anual de la producătorul licențelor de tip Annual Software Subscription & Support Renewal 12 Months, sau echivalentul, pentru perioada 01.11.2020 - 31.10.2021, a instrumentului exploatat în cadrul Sistemului Informațional al BNM cu următoarea componență: - IBM Security QRadar SIEM All-in-One Virtual 3190 Install (licență de bază) – 1 buc. IBM Security QRadar Virtual SIEM Event Capacity Increase of 100 EPS Install (pachete adiționale) – 9 buc. Termen de prestare: Confirmarea prestării serviciilor trebuie să fie prezentată obligator în perioada 01.10.2020 - 30.10.2020 inclusiv, și va include: - furnizarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau - publicarea informației confirmative pe site-ul producătorului.		Nu se aplică
72267 000-4	Servicii de asigurare a accesului la menținerea				Tip: Serviciile de asigurare a accesului la suport anual de la producătorul licențelor de tip Annual Software Subscription & Support Renewal 12 Months, sau echivalentul, a modulului IBM		

	anuală a modulului IBM Security QRadar Vulnerability Manager				Security QRadar Vulnerability Manager, trebuie să fie egalată cu perioada de suport pentru Instrumentul IBM Security Qradar indicat la prima poziție, până la 31.10.2021, cu următoarea componență: • IBM QRadar Software Node Install License - 1 licență pentru consola de roluri de software • IBM Security QRadar Vulnerability Manager Software 60XX Install License - 1 licență pentru scanarea la vulnerabilități a 256 resurse informaționale (assets) și managementul de configurare standard a 50 de resurse Termen de prestare: Confirmarea prestării serviciilor trebuie să fie prezentată obligator în perioada 01.10.2020 - 30.10.2020 inclusiv, și va include: - furnizarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau - publicarea informației confirmative pe site-ul producătorului.		
Lotul 4: Soluție integrată pentru gestionarea aplicațiilor și dispozitivelor mobile							
48730 000-4	Soluție integrată pentru gestionarea aplicațiilor și dispozitivelor mobile, cu 12 luni suport standard de la Producător inclus				Tip: Licență pentru soluția integrată pentru gestionarea aplicațiilor și dispozitivelor mobile pentru 50 utilizatori, cu 12 luni suport standard de la Producător inclus, care să cuprindă tehnologii moderne pentru gestionarea aplicațiilor și dispozitivelor mobile cu un grad de protecție ridicat. Cantitate: Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul asigurarea cu licență pentru 50 utilizatori cu posibilitatea asignării până la 5 dispozitive per utilizator precum și posibilitatea extinderii ulterioare a numărului de licențe. Nota: Ofertantul va veni cu o soluție care va acoperi partea de software necesară pentru întreaga soluție cu respectarea cerințelor specificate mai jos: Cerințe tehnice și specifice: Sistemul propus trebuie să fie o soluție inovatoare, care să asigure următoarele cerințe:		Nu se aplică

					1. Cerințe pentru Securitatea datelor corporative: • Controlul securizat al accesului la datele corporative; • Autentificare bifactorială la datele corporative; • Prevenirea pierderilor de date (DLP); • Posibilitatea de implementare a politicilor de criptare (dispozitiv, SD); • Posibilitatea de securizare și control pentru E-mail și DLP: - Control asupra atașamentelor email; - Control asupra datelor inserate sau copiate; • Posibilitatea de securizare și control al browser-ului mobil; • Posibilitatea de ștergere condiționată a datelor corporative de pe dispozitivele mobile; • Posibilitatea de a lucra offline (nu necesită o conexiune permanentă la server pentru identificarea și eliminarea amenințărilor pe dispozitive); • Partajarea datelor corporative de cele personale (BYOD); • Posibilitatea de creare a canalului VPN securizat per aplicație (inclusiv Windows); 2. Cerințe pentru Managementul Aplicațiilor: • Identificarea aplicațiilor mobile instalate și posibilitatea de distribuție a aplicațiilor noi; • Posibilitatea de categorizare a aplicațiilor mobile; • Posibilitatea de creare a listelor admise/interzise de aplicații mobile; • Posibilitatea de creare a restricțiilor pentru rețele wifi • Managementul aplicațiilor mobile (magazine intern de aplicații mobile); • Publicare și livrare centralizată sigură a aplicațiilor mobile; • Containerizarea aplicațiilor mobile; 3. Cerințe pentru Managementul dispozitivelor; • Posibilitatea de încadrare a dispozitivelor mobile personale, în mediul corporativ (BYOD); • Posibilitatea utilizatorilor de auto-înrolare a dispozitivelor mobile (self-service) în sistem; • Posibilitatea de integrare a soluției cu infrastructura		
--	--	--	--	--	---	--	--

					<i>existentă a întreprinderii;</i> - <i>Active Directory;</i> - <i>Aplicații interne a companiei (aplicații Web, Mobile);</i> - <i>FileServer;</i> - <i>SIEM;</i> • <i>Managementul conținutului dispozitivului mobil;</i> • <i>Managementul dispozitivelor mobile;</i> • <i>Posibilitatea de creare a modului de lucru KIOSK;</i> • <i>Geo-localizarea dispozitivelor mobile;</i> • <i>Suport pentru o gamă extinsă de platforme:</i> - <i>Windows 10 Desktop;</i> - <i>MacOS;</i> - <i>Android;</i> - <i>iOS;</i> • <i>Sistemul trebuie să ofere funcții avansate de gestionare pentru PC-urile Windows 10 precum:</i> - <i>personalizarea aspectului sistemului;</i> - <i>executarea scripturilor PowerShell (.ps1);</i> - <i>executarea de scripturi pentru modificarea registrului (.reg);</i> - <i>setarea BitLocker pentru criptarea discului;</i> - <i>gestionarea drepturilor utilizatorului;</i> - <i>setarea accesului la funcțiile Windows (meniul de setări);</i> - <i>instalarea oricărui GPO prin registru;</i> - <i>gestionarea sistemului de fișiere;</i> - <i>instalarea de drivere;</i> - <i>instalarea aplicațiilor LOB;</i> - <i>instalarea pachetelor software;</i> - <i>dezinstalarea software-ului preinstalat;</i> - <i>gestionarea imprimantei, etc.;</i> 4. Cerințe pentru Serverul de administrare: • <i>Instalarea componentelor serverului soluției nu trebuie să necesite preinstalarea unui sistem de operare separat și a unei baze de date separate, precum și a licențelor lor separate</i> • <i>Posibilitatea de a instala componente suplimentare de</i>		
--	--	--	--	--	---	--	--

					server: - pentru a asigura funcționarea sistemului cu disponibilitate ridicată (high availability) - posibilitatea utilizării în scopuri de testare înainte de a adăuga orice funcționalitate în mediul de lucru • Soluția trebuie să asigure extinderea cu ușurință a dispozitivelor gestionate • Posibilitatea de update a soluției direct din consola de administrare, fără implicarea directă a producătorului • Android Enterprise suport pentru dispozitivele BYOD 5. Certificări conform standardelor internaționale: • FIPS 140-2; • ISO/IEC 27001:2013; • Common Criteria Certification; Cerința de certificare poate fi demonstrată prin prezentarea copiei certificatului, sau referință pe site-ul producătorului. Alte cerințe obligatorii: <u>Perioada de suport și mentenanță de la producător:</u> 1. Pentru soluția oferită se solicită a fi pentru o perioadă de 12 luni din data acceptanței soluției. 2. Producătorul trebuie să ofere: - suport 24/24, prin e-mail sau conectare de la distanță, - asigurarea accesului la update-uri și Baza de cunoștințe (Knowledge Base + Product Updates) <u>Notă:</u> Lucrările de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției precum și transferul de cunoștințe trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă. Termen de livrare: 30 de zile lucrătoare din data intrării în vigoare a contractului care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.		
--	--	--	--	--	---	--	--

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]

Numărul procedurii de achiziție nr. ocds-b3wdp1-MD-1597044662049 din 07.09.2020

Denumirea procedurii de achiziție: *Pachete software aferente securității informaționale*

Cod CPV	Denumirea bunurilor	Unitatea de măsură	Cantitatea	Preț unitar (fără TVA)	Preț unitar (cu TVA)	Suma (fără TVA)	Suma (cu TVA)	Termenul de livrare	Clasificația bugetară (IBAN)
1	2	3	4	5	6	7	8	9	10
Lotul 1: Soluție de protecție, securitate, patch management și disk encryption pentru locurile de muncă									
48760000-3	Soluție de protecție, securitate, patch management si disk encryption pentru locurile de muncă	buc.	1					Toate bunurile/serviciile vor fi livrate și/sau prestate de către Vânzător/Prestator la sediul Cumpărătorului/Beneficiarului în termenele indicate pe fiecare lot în parte. Vânzătorul/Prestatorul va asigura livrarea bunurilor și/sau prestarea serviciilor în corespundere cu toate cerințele înaintate.	Nu se aplică
Total lot 1									
Lotul 2: Menținerea licențelor McAfee									
72268000-1	Servicii de asigurare a accesului la suport anual Business Support, sau echivalentul, pentru licențe McAfee Total Protection for Data Loss Prevention	buc.	1					Toate bunurile/serviciile vor fi livrate și/sau prestate de către Vânzător/Prestator la sediul Cumpărătorului/Beneficiarului în termenele indicate pe fiecare lot în parte. Vânzătorul/Prestatorul va asigura livrarea bunurilor și/sau prestarea serviciilor în corespundere cu toate cerințele	Nu se aplică

	Software, pentru 400 licențe							înaintate.	
48219100-7	Subscriere anuală pentru licența McAfee Web Protection, inclusiv 1 an de suport anual Business Support, sau echivalentul, pentru 400 utilizatori	buc.	1						
Total lot 2									
Lotul 3: Menținerea soluției IBM Qradar									
72267000-4	Servicii de asigurare a accesului la menținerea anuală a instrumentului IBM Security Qradar	buc.	1					Toate bunurile/serviciile vor fi livrate și/sau prestate de către Vânzător/Prestator la sediul Cumpărătorului/Beneficiarului în termenele indicate pe fiecare lot în parte. Vânzătorul/Prestatorul va asigura livrarea bunurilor și/sau prestarea serviciilor în corespundere cu toate cerințele înaintate.	Nu se aplică
72267000-4	Servicii de asigurare a accesului la menținerea anuală a modulului IBM Security QRadar Vulnerability Manager	buc.	1						
Total lot 3									
Lotul 4: Soluție integrată pentru gestionarea aplicațiilor și dispozitivelor mobile									
48730000-4	Soluție integrată pentru gestionarea aplicațiilor și dispozitivelor mobile, cu 12 luni suport standard de	buc.	1					Toate bunurile/serviciile vor fi livrate și/sau prestate de către Vânzător/Prestator la sediul Cumpărătorului/Beneficiarului în termenele indicate pe fiecare lot în parte.	Nu se aplică

	la Producător inclus							<i>Vânzătorul/Prestatorul va asigura livrarea bunurilor și/sau prestarea serviciilor în corespundere cu toate cerințele înaintate.</i>	
Total lot 4									
TOTAL									

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

Ofertantul: _____ Adresa: _____

CAPITOLUL 5
FORMULARUL DE CONTRACT

Formular	Denumirea
F5.1	Contract-model



ACHIZIȚII PUBLICE

CONTRACT nr. _____
de achiziționare prin procedura de _____
Cod CPV: 48730000-4

” ” 20 _____

mun. Chișinău

Furnizor de bunuri	Autoritatea contractantă
_____, (denumirea completă a întreprinderii, asociației, organizației) reprezentată prin _____, (funcția, numele, prenumele) care acționează în baza _____, (statut, regulament, hotărâre etc.) denumit(a) în continuare Vânzător, _____, (se indică nr. și data de înregistrare în Registrul de Stat) pe de o parte,	BANCA NAȚIONALĂ A MOLDOVEI, reprezentată prin viceguvernatorul dl _____, (funcția, numele, prenumele) care acționează în baza Legii cu privire la Banca Națională a Moldovei nr.548/1995, cu modificările ulterioare, denumită în continuare Beneficiar, pe de o parte,

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

- Achiziționarea _____, denumite în continuare Bunuri/Servicii, conform procedurii de achiziții publice de tip licitație deschisă din _____, în baza deciziei grupului de lucru al BĂNCII NAȚIONALE A MOLDOVEI din _____.
- Următoarele documente vor fi considerate părți componente și integrale ale Contractului:
 - Anexa nr. 1: Specificația Bunurilor/Serviciilor.
- Prezentul Contract va predomina asupra tuturor altor documente componente. În cazul unor discrepanțe sau inconsecvențe între documentele componente ale Contractului, documentele prevăzute la lit.b vor avea ordinea de prioritate enumerată mai sus.
- În calitate de contravaloare a plăților care urmează a fi efectuate de Cumpărător/Beneficiar, Vânzătorul/Prestatorul se obligă prin prezenta să presteze Cumpărătorului/Beneficiarului Bunurile/Serviciile în conformitate cu prevederile Contractului sub toate aspectele.
- Cumpărătorul/Beneficiarul se obligă prin prezenta să plătească Vânzătorului/Prestatorului, în calitate de contravaloare a livrării Bunurilor/prestării Serviciilor, precum și a înlăturării defectelor lor, prețul Contractului sau orice altă sumă care poate deveni plătitibilă conform prevederilor Contractului în termenele și modalitatea stabilite de Contract.

1. Obiectul Contractului

- Vânzătorul/Prestatorul își asumă obligația de a livra Bunurile/presta Serviciile prevăzute în Anexa nr. 1, care este parte integrantă a prezentului Contract.
- Cumpărătorul/Beneficiarul se obligă, la rândul său, să achite și să recepționeze Bunurile livrate/Serviciile prestate de Vânzător/Prestator.

2. Termeni și condiții de livrare și/sau prestare

2.1. Livrarea Bunurilor și/sau Prestarea Serviciilor se efectuează de către Vânzător/Prestator la adresa Beneficiarului: MD-2005, mun. Chișinău, bd. Grigore Vieru 1, BANCA NAȚIONALĂ A MOLDOVEI în termen de până la _____ inclusiv.

2.2. Documentația de însoțire a Bunurilor/Serviciilor include:

- a) Factura fiscală;
- b) Actul de predare-primire a Bunurilor și/sau Serviciilor.

2.3. Originalele documentelor prevăzute în pct. 2.2 se vor prezenta Cumpărătorului/Beneficiarului la momentul livrării Bunurilor și/sau prestării Serviciilor la sediul Cumpărătorului/Beneficiarului. Livrarea Bunurilor și/sau Serviciilor se consideră încheiată din momentul în care sunt prezentate și aprobate documentele din pct. 2.2.

3. Prețul și condiții de plată

3.1. Prețul Bunurilor livrate și/sau Serviciilor prestate conform prezentului Contract este stabilit în lei moldovenești, fiind indicat Anexa nr. 1 a prezentului Contract.

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

3.3. Achitarea plăților pentru Bunurile livrate și/sau Serviciile prestate se va efectua în lei moldovenești.

3.4. Cumpărătorul/Beneficiarul achită Bunurile/Serviciile specificate în Anexa nr. 1 a prezentului Contract după livrarea Bunurilor și/sau prestarea Serviciilor în baza actului de predare-primire a Bunurilor și /sau Serviciilor, semnat de reprezentanții ambelor Părți și a facturii fiscale prezentate de către Vânzător/Prestator, în decurs de 15 zile lucrătoare de la data recepționării documentelor de către Cumpărător/Beneficiar.

3.5. Plățile se vor efectua prin transfer bancar pe contul Vânzătorului/Prestatorului indicat în prezentul Contract.

3.6. Vânzătorul/Prestatorul are obligația întocmirii corecte a facturii fiscale, indicând toate elementele de identificare ale acesteia și datele bancare corecte, inclusiv ale Cumpărătorului/Beneficiarului.

3.7. Transmiterea documentelor enumerate la pct. 2.2 cu elemente greșite și/sau greșeli de calcul, identificate de Cumpărător/Beneficiar, urmare recepționării acesteia, atrage după sine obligația Vânzătorului/Prestatorului de a le anula și de a transmite documente noi.

4. Condiții de predare-primire

4.1. Bunurile și/sau Serviciile se consideră predate de către Vânzător/Prestator și recepționate de către Cumpărător/Beneficiar dacă cantitatea Bunurilor livrate și/sau volumul Serviciilor prestate corespunde prevederilor din Anexa nr. 1 a prezentului Contract și documentelor de însoțire a Bunurilor și/sau Serviciilor conform pct. 2.2. al prezentului Contract, *inclusiv a fost prezentată de către Prestator a unui document confirmativ parvenit de la compania producător/filiala companiei producător sau confirmarea înregistrată pe site-ul producătorului, ce să garanteze disponibilitatea pentru Beneficiar a serviciilor de suport anual conform Anexei nr. 1 a prezentului Contract (după caz).*

4.2. Vânzătorul/Prestatorul este obligat să prezinte Cumpărătorului/Beneficiarului originalele documentației specificate în pct. 2.2. al prezentului Contract odată cu livrarea Bunurilor și/sau prestarea Serviciilor, pentru efectuarea plății. Pentru nerespectarea de către Vânzător/Prestator a prezentei clauze, Cumpărătorul/Beneficiarul își rezervă dreptul de a majora termenul de achitare prevăzut în pct. 3.4 corespunzător numărului de zile lucrătoare de întârziere și de a fi exonerat de achitarea penalității stabilite în pct. 10.4. al prezentului Contract.

5. Standarde

5.1. Bunurile livrate și/sau Serviciile prestate în baza Contractului vor respecta standardele prezentate de către Vânzător/Prestator în propunerea sa tehnică.

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 și/sau Serviciilor.

6. Obligațiile părților

6.1. În baza prezentului Contract, Vânzătorul/Prestatorul se obligă:

- a. să livreze Bunurile și/sau presteze Serviciile în condițiile prevăzute de prezentul Contract;
- b. să anunțe Cumpărătorul/Beneficiarul după semnarea prezentului Contract, în decurs de 5 zile calendaristice, prin telefon/fax, e-mail sau telegramă autorizată, despre disponibilitatea livrării Bunurilor și/sau prestării Serviciilor;
- c. să asigure condițiile corespunzătoare pentru recepționarea Bunurilor și/sau Serviciilor de către Cumpărător/Beneficiar, în termenele stabilite, în corespundere cu cerințele prezentului Contract;
- d. să asigure integritatea și calitatea Bunurilor și/sau Serviciilor pe toată perioada de până la recepționarea lor de către Cumpărător/Beneficiar
- e. *să execute lucrările de instalare, configurare și punerea în funcțiune a soluției (după caz).*

6.2. În baza prezentului Contract, Cumpărătorul/Beneficiarul se obligă:

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

7. Forța majoră

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

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

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

7.4. Suspendarea temporară și reluarea livrării bunurilor și/sau prestării Serviciilor, se efectuează în baza proceselor verbale semnate de către Părți.

8. Rezoluțiunea

8.1. Rezoluțiunea Contractului se poate realiza cu acordul comun al Părților.

8.2. Contractul poate fi rezoluționat în mod unilateral de către:

- a. Cumpărător/Beneficiar în caz de refuz al Vânzătorului/Prestatorului de a livra Bunurile și/sau presta Serviciile prevăzute în prezentul Contract;
- b. Cumpărător/Beneficiar în caz de nerespectare de către Cumpărător/Prestator a termenelor de livrare și/sau prestare stabilite;
- c. Vânzător/Prestator în caz de nerespectare de către Cumpărător/Beneficiar a termenelor de plată a Bunurilor și/sau Serviciilor;
- d. Vânzător/Prestator sau Cumpărător/Beneficiar 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 zile lucrătoare celeilalte Părți despre intențiile ei printr-o scrisoare motivată.

8.4. Partea înștiințată este obligată să răspundă în decurs de 5 zile lucrătoare de la primirea notificării. În cazul în care litigiul nu este soluționat în termenele stabilite, Partea inițiatore va iniția rezoluția.

9. Reclamații

9.1. Reclamațiile privind cantitatea Bunurilor livrate și/sau volumul Serviciilor prestate sunt înaintate Vânzătorului/Prestatorului la momentul recepționării lor, fiind confirmate printr-un act întocmit în comun cu reprezentantul Vânzătorului/Prestatorului.

9.2. Pretențiile privind calitatea Bunurilor livrate și/sau Serviciilor prestate sunt înaintate Vânzătorului/Prestatorului în termen de 5 zile lucrătoare de la depistarea deficiențelor de calitate.

9.3. Vânzătorul/Prestatorul este obligat să examineze pretențiile înaintate în termen de 5 zile lucrătoare de la data primirii acestora și să comunice Cumpărătorului/Beneficiarului despre decizia luată.

9.4. Vânzătorul/Prestatorul este obligat, în termen de 5 zile lucrătoare, să livreze și/sau să presteze suplimentar Cumpărătorului/Beneficiarului cantitatea nelivrată de Bunuri și/sau volumul neprestat de Servicii, iar în caz de constatare a calității necorespunzătoare – să le substituie sau să le corecteze în conformitate cu cerințele Contractului.

9.5. Vânzătorul/Prestatorul poartă răspundere pentru calitatea Bunurilor și/sau Serviciilor în limitele stabilite, inclusiv pentru viciile ascunse.

10. Sancțiuni

10.1. Forma de garanție de bună executare a Contractului agreată de Cumpărător/Beneficiar este garanția bancară, în cuantum de 5% din valoarea Contractului. Termenul de valabilitate al garanției bancare va depăși cu cel puțin 30 zile calendaristice data planificată a semnării Actului de primire-predare a Bunurilor și/sau Serviciilor.

10.2. Pentru refuzul de a livra Bunurile și/sau presta Serviciile prevăzute în prezentul Contract, se va reține garanția de bună executare a Contractului.

10.3. Pentru livrarea cu întârziere a Bunurilor și/sau prestarea cu întârziere a Serviciilor, Vânzătorul/Prestatorul poartă răspundere materială în valoare de 0,1% din suma Bunurilor și/sau Serviciilor prestate cu întârziere, pentru fiecare zi lucrătoare de întârziere, dar nu mai mult de 5 % din suma totală a prezentului Contract. În cazul în care întârzierea depășește 25 zile calendaristice, Vânzătorul/Prestatorul prezintă Cumpărătorului/Beneficiarului o explicație în formă scrisă și prelungește termenul de valabilitate a garanției de bună executare, în caz contrar se consideră ca fiind refuz de a livra Bunurile și/sau presta Serviciile prevăzute în prezentul Contract și Vânzătorului/Prestatorului i se va reține garanția de bună executare a Contractului.

10.4. Pentru achitarea cu întârziere, Cumpărătorul/Beneficiarul poartă răspundere materială în valoare de 0,1% din suma Bunurilor și/sau Serviciilor achitate cu întârziere, pentru fiecare zi lucrătoare de întârziere, dar nu mai mult de 5% din suma totală a prezentului Contract.

10.5. Prima zi lucrătoare ulterioară datei ce constituie termenul limită de prestare/ de achitare se consideră zi lucrătoare de întârziere.

10.6. Suma penalității calculate Vânzătorului/Prestatorului conform prezentului Contract poate fi dedusă (reținută) de către Cumpărător/Beneficiar din suma plății pentru Bunurile livrate și/sau Serviciile prestate.

11. Drepturi de proprietate intelectuală

11.1. Vânzătorul/Prestatorul are obligația să despăgubească Cumpărătorul/Beneficiarul împotriva oricărui:

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

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

12. Confidențialitate

- 12.1. Toată informația furnizată de către o Parte către cealaltă Parte în vederea executării prezentului Contract se consideră a fi confidențială, dacă nu este stabilit expres de către Partea care dezvăluie că informația dată este publică.
- 12.2. Niciuna dintre Părți nu are dreptul să utilizeze sau să facă publică nici o informație confidențială aferentă serviciilor prestate, activității celeilalte Părți, primite de la cealaltă Parte sau din alte surse prevăzute în prezentul Contract, cu excepția informației asupra căreia cealaltă Parte își dă acordul scris în vederea divulgării acesteia.
- 12.3. Fiecare Parte își asumă responsabilitatea ca fiecare persoană implicată în prestarea Serviciilor prevăzute în prezentul Contract să respecte obligatoriu următoarele condiții de păstrare a confidențialității informației:
- a. să nu divulge, transmită sau să utilizeze în interesul oricărei alte persoane în afară de cealaltă Parte sau persoanele împuternicite de aceasta, nici o informație cu caracter confidențial sau material pe care el sau ea îl va primi de la cealaltă Parte, cu excepția materialelor sau informației aflate anterior în evidența acestei persoane sau care s-ar putea să fi fost obținută înaintea unei astfel de divulgări, transmiteri sau utilizări de la persoane terțe sau din sectorul public;
 - b. să respecte toate politicile sau indicațiile date de cealaltă Parte în ceea ce privește asigurarea securității informației, clasificarea, utilizarea sau dispunerea oricărei informații cu acces limitat sau cu caracter confidențial prin semnarea în acest sens a unui angajament de respectare a cerințelor de securitate de către fiecare reprezentant delegat al acestei Părți;
 - c. să nu folosească nici o informație cu acces limitat sau cu caracter confidențial pentru obținerea unui beneficiu personal.
- 12.4. Fiecare Parte este obligată să respecte confidențialitatea privind metodologiile/ instrumentele/ tehnicile aplicate de cealaltă Parte în prestarea Serviciilor, cu excepția celor publice.
- 12.5. Părțile nu vor dezvălui, publica și răspândi informațiile confidențiale nimănui altcuiva decât angajaților proprii care au nevoie să cunoască aceste informații. Dacă este necesară implicarea unei terțe părți (companii de consultanță sau subcontractori), aceasta se va face cu acordul celeilalte Părți și urmând a fi încheiate acorduri de confidențialitate înaintea autorizării oricărei terțe Părți.
- 12.6. Părțile vor limita accesul la asemenea informații confidențiale pentru angajații, funcționarii și managerii lor care au nevoie să le cunoască, și vor informa aceste persoane asupra obligațiilor asumate prin acest Contract.
- 12.7. Fiecare Parte va păstra în deplină securitate toate suporturile materiale de stocare transmise și care conțin informațiile ce aparțin celeilalte Părți, oricare ar fi forma de păstrare sau înregistrare a acestora.

12.8.Orice pierdere sau suspiciune de pierdere a oricărui document ce conține informații confidențiale va fi anunțată imediat de către Partea care a depistat pierderea respectivă.

12.9.La cererea uneia dintre Părți, cealaltă Parte este obligată să-i înapoieze acesteia toate suporturile materiale (de stocare) ce conțin informații confidențiale, inclusiv orice copie făcută după acestea, iar orice informație ce se află pe suportul ce nu poate fi distrusă va fi ștearsă.

12.10.Toate obligațiile create prin acest capitol vor continua și după schimbarea sau terminarea relației de afaceri dintre Părți pe o perioadă nelimitată.

13. Dispoziții finale

13.1. 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 Republicii Moldova.

13.2. Părțile contractante au dreptul, pe durata îndeplinirii Contractului, să convină asupra modificării clauzelor Contractului, prin act 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 ambele Părți.

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

13.4. Prezentul Contract este întocmit în două exemplare în limba de română, câte un exemplar pentru Prestator și Beneficiar.

13.5. Prezentul Contract se consideră încheiat și intră în vigoare la data semnării lui de către Părți, fiind valabil până la 31 decembrie 2020 (*după caz*), cu excepția drepturilor și obligațiilor aplicabile Părților pe parcursul perioadei indicate în Anexa nr. 1, care rămân valabile până la finele perioadei respective.

13.6. Prezentul Contract reprezintă acordul de voință al Părților și se consideră semnat la data aplicării ultimei semnături de către una din Părți.

13.7. Pentru confirmarea celor menționate mai sus, Părțile au semnat prezentul Contract în conformitate cu legislația Republicii Moldova, la data și anul indicate mai sus.

14. Datele juridice, poștale și bancare ale Părților

Furnizorul de Bunuri/Prestatorul de Servicii	Autoritatea contractantă
Adresa poștală: Telefon: IBAN: Banca: Adresa poștală a băncii: Cod: Cod fiscal:	Adresa poștală: Telefon: IBAN: Banca: Adresa poștală a băncii: Cod: Cod fiscal:

Semnăturile părților

Furnizorul de Bunuri/Prestatorul de Servicii	Autoritatea contractantă
Semnătura autorizată: L.Ș.	Semnătura autorizată: L.Ș.