ANUNȚ DE PARTICIPARE

privind achiziționarea pachetelor software aferente securității informaționale
prin procedura de achiziție: Licitație deschisă

1. **Denumirea autorității contractante: Banca Națională a Moldovei**
2. **IDNO: 79592**
3. **Adresa: MD-2005, bulevardul Grigore Vieru 1**
4. **Numărul de telefon/fax: 022 822259 / 022 228338**
5. **Adresa de e-mail și de internet a autorității contractante: official@bnm.md, www.bnm.md**
6. **Adresa de e-mail sau de internet de la care se va putea obține accesul la documentația de atribuire: *documentația de atribuire este anexată în cadrul procedurii în SIA RSAP* „M-Tender”.**
7. **Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind achiziționarea următoarelor bunuri:**

Nr. d/o	Cod CPV	Denumirea bunurilor solicitate	Unitatea de măsură	Canti-tatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimativă MDL, fără TVA
Lotul 1: Soluție de protecție, securitate, patch management si disk encryption pentru locurile de muncă						**211 666,67**
1	48760000-3	Soluție de protecție, securitate, patch management și disk encryption pentru locurile de muncă	buc	1	*<u>Tip</u>: Subscriere anuală pentru soluția de protecție și securitate Bitdefender GravityZone Elite, sau echivalentul, pentru 530 locuri de muncă (PC/laptop/VDI) și 750 căsuțe poștale pentru perioada 12.01.2020-12.01.2021).* *<u>Cantitate:</u> Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul:* *- 530 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.* • *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. *permită vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi si îmbunătățiri, probleme rezolvate, probleme cunoscute* 5. *afișeze notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție viruși, actualizări de produs disponibile).* 6. *permită integrarea cu un server Syslog pentru raportarea evenimentelor antivirus.*	

					7. *permită instalarea serviciului de SMNP pentru raportarea statusului mașinilor din cadrul componentei de management.* 8. *permită crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programat, stocata local, pe un server FTP sau în rețea.* ***<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 si 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 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 directoy.*	

					- *poată fi schimbată automat în funcție de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este în accesai rețea cu infrastructura de management, Tipul rețelei (lan, wireless).* ***<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.* - *trimită 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.* ***Log-uri:*** - *Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare.* ***Protecție stații și servere fizice si virtualizate – caracteristici minime:*** *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 daca 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 siguranța. Pentru acțiunea implicită: doar raportare, dezinfecție, ștergere și transmitere în carantină. Pentru acțiunea de siguranța: ștergere sau permutare în carantină* ***Cerințe de sistem:*** - *Sisteme de operare pentru stații de lucru: Windows 10/8.1,7, Vista (SP1), XP (SP3), Mac OS X 10.12.x, 10.11.x, 10.10.x ,10.9.x, 10.8.x .* - *Sisteme de operare Windows pentru servere: Windows Server 2003/2008/2008 R2/2012/2012 R2/2016.* - *Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Oracle Linux 6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual, Debian 5.0 sau mai recent.* ***Administrare și instalare remote:***	

					- *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 decît cele integrate în domen.* ***<u>Caracteristici și funcționalități principale ale modulului antivirus</u>*** *Produsul trebuie sa 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 virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansata 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 bazatte 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 in 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.* ***Firewall:*** - *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.* ***Protecția datelor:*** - *Produsul trebuie să permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.* ***Controlul conținutului:*** *Produsul trebuie să ofere un modul integrat dedicat controlului accesului la Internet cu următoarele particularități: blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini, blocarea accesului la Internet pe intervale orare, blocarea paginilor de internet care conțin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, blocarea accesului la anumite aplicații definite de administrator, restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).* ***Controlul aplicațiilor:*** *Pentru administrare și inventariere eficientă produsul trebuie să dețină un modul care va oferi posibilitatea de a:* - *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 subprocese) după: cale fișier: local, CD-ROM, portabil sau rețea, hash , certificat.* ***Controlul dispozitivelor:*** *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.* ***Power User:*** *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 suprascrie din consola setările aplicate de utilizatorii Power User.* ***Actualizare:*** *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.* ***Protecție și securitate pentru telefoane mobile de tip smartphone:*** *Produsul trebuie să ofere client de protecție pentru dispozitive mobile cu platforma Android (de la v. 2.2) și iOS (de la v 5.)* *Clientul mobil trebuie să:* - *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>*** *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 si la cerere.* - *includă, pe lîngă detecția pe baza de semnături, scanarea euristică comportamentală pentru a proteja sistemul de virușii 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 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 atît referitoare la scanarea antivirus cît 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.* **- (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, CitrixȘ 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)* ***<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 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 sistemei 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 local și menținere de la producător:</u>* *1. Pentru soluția ofertată se solicită a fi 12 luni pentru perioada 12.01.2020-12.01.2021.* *2. Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului.* *<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 01.12.2019 - 26.12.2019, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.*	
Lotul 2: Extinderea și menținerea licențelor McAfee						**428 333,33**
1	48732000-8	Licență pentru 50 utilizatori pentru soluția de prevenire a scurgerii de informație McAfee Total Protection For Data Loss Prevention Appliance Software, sau echivalentul, inclusiv 1 an de suport standard	buc	1	***Tip:** Soluție de prevenire în mod automatizat a scurgerii de informații clasificate ale BNM și sporirea controlului asupra datelor în cadrul BNM (DLP - Data Loss Prevention), care va include control pentru:* *- Stații de lucru (endpoint)* *- Serviciul proxy (iCap)* *- Serviciul de poștă electronica (SMTP)* *- Monitorizarea rețelei (Network monitor).* ***Cantitate:** licență pentru 50 utilizatori.* ***<u>Condiții generale:</u>*** *Se solicită extinderea numărului de licențe McAfee Total Protection For Data Loss Prevention Appliance Software, sau echivalentul, inclusiv un an de suport, pentru 50 utilizatori.* *<u>Notă:</u> Luând în considerație că în BNM sunt deja în exploatare licențe pentru 350 utilizatori, în caz de oferire a altui produs decât McAfee DLP, Ofertantul trebuie să acopere cu licență pentru toți 400 utilizatori (50 noi + 350 existente pentru care se solicită menținerea în poziția 2). Totodată, va fi responsabil pentru livrarea, instalarea, configurarea (inclusiv configurarea politicilor inițiale) și punerea în funcțiune a soluției și pentru asigurarea suportului la definirea/configurarea și exploatarea soluției pentru primul an de exploatare a acesteia.* ***<u>Caracteristici generale:</u>*** *<u>Protecție Endpoint:</u>*	

					- *să suporte sistemele de operare: Microsoft Windows 7 (32/64-bit), Microsoft Windows 8.1 (32/64-bit), Microsoft Windows 10 (32/64-bit).* - *să identifice conținutul chiar dacă acesta este arhivat (minimum 10 niveluri de arhivare).* - *să poată aplica politici bazate pe conținut confidențial pentru cel putin 300 de tipuri de fișiere.* - *să poată detecta documentele ce au fost clasificate deja (fie prin intermeniul unui instrument de clasificare a documentelor prin înscrierea în Metadate și/sau prin aplicare de marcări vizuale, fie prin faptul că documentul dat conține careva marcaje vizuale cu privire la clasa căreia aparține (ex. mențiuni în header/footer pentru documente word) sau în funcție de sursa documentului - aplicația prin intermediul căreia a fost creat).* - *agentul soluției să poată proteja minim 100.000 de documente indiferent dacă stația este Online sau Offline;* - *analiza conținutului să nu fie limitată la limba utilizată;* - *soluția trebuie să permită parametrizarea nivelului de utilizare a resurselor utilizate (procesor, RAM);* - *să protejeze informația confidențială la:* - *scrierea pe suporturi de stocare mobile (memorii USB, optice etc.);* - *trimisă prin intermediul serviciilor de poștă electronică;* - *încărcată pe web;* - *copiată cu ajutorul clipboard-ului;* - *printată în fișier sau pe imprimantă;* - *scrisă pe un share în rețea;* - *folosită în aplicațiile network–based;* - *la efectuarea screenshot–ului ecranului.* - *să mențină înregistrări de audit privind activitatea agentului de endpoint;* - *să mențină înregistrări de audit privind activitatea agentului de endpoint;* - *soluția trebuie să dispună de mecanisme proprii de instalare a agenților pe stațiile de lucru sau alte sisteme, sau să permită integrarea cu Directory Services;* - *agentul de endpoint trebuie să fie compatibil, determinat prin testări, cu soluții de antivirus, firewall, criptare, backup și antispyware third-party;* - *agentul de endpoint trebuie să permită aplicarea politicilor folosind conținut înregistrat/ amprentat;* - *agentul de endpoint trebuie să aibă opțiunea de blocare a activității pentru situațiile de încălcare a politicii de securitate prestabilită (ex. - se încearcă upload-area de documente considerate confidențiale; - copierea pe SD card, USB flash drive / memory stick; - crearea de noi documente pe baza celor originale; - crearea de arhive și upload-area ulterioară a acestora (sau copierea pe USB flash);* - *construirea regulilor de protecție trebuie să se poată face și în funcție de cuvinte-cheie, expresii regulate și amprente (hash-uri);*	

					- *construcția regulilor trebuie să includă suport pentru logica booleana incluzând AND, OR, sau alte declarații logice;* - *soluția trebuie să aibă abilitatea de a identifica fișierele bazându-se pe conceptul de true file type și nu doar pe extensia fișierelor;* - *trebuie să poată scana stația și să identifice documentele ce conțin informații clasificate (funcții de tipul descoperă - discovery);* - *să permită efectuarea de notificări customizate;* - *trebuie să fie capabilă să identifice nivelul de clasificare a documentelor din marcajele vizuale și să aplice regulile de protectie pe aceste documente.;* - *trebuie să fie capabilă să protejeze documente nemarcate ce au conținut ce provine din documente clasificate cu marcaje vizuale.* - *soluția trebuie să permită creare de politici în mod granular de permitere / blocare a dispozitivelor periferice pe baza informațiilor despre:* a. *ID Producator* b. *ID Model Dispozitiv Periferic* c. *Tipul de dispozitiv* d. *Clasa dispozitivului detectat de sistemul de operare* e. *BUS Conectare (USB, S-ATA, ETC.)* f. *Numele Dispozitivului* g. *Tipul sistemului de fișiere (NTFS/FAT/FAT32)* h. *Numele Volumului / Partiției (în cazul dispozitivelor de stocare date)* - *soluția trebuie să poată lua urmatoarele acțiuni la conectarea unui dispozitiv periferic:* a. *blocare: să nu permită instalarea acestuia;* b. *monitorizare: să genereze un eveniment ce conține detalii despre dispozitiv;* c. *forțare mod utilizare ReadOnly: în cazul dispozitivelor de stocare date, acestea se vor utiliza doar pentru citirea datelor de pe ele.* d. *soluția trebuie sa poata prevenii executarea de cod si aplicatii direct de pe dispozitive externe. De asemenea, trebuie sa vina si cu un mecanism de macare a aplicatiilor permise.* - *soluția trebuie să permită aplicarea de politici diferite în funcție de locația utilizatorlui (ex: să nu poată conecta imprimante atunci când nu se află în perimetrul rețelei).* - *soluția trebuie să ofere un mecanism de dezactivare a restricțiilor pentru utilizatorii ce nu au conectivitate cu severul de administrare.* - *soluția trebuie să permită construirea unei liste de dispozitive permise și corelarea acestei liste la utilizatori / grupuri de utilizatori din Directory Services, astfel încât aceștia să poată utiliza dispozitivele indiferent de calculatorul la care se afla.* - *soluția trebuie să permită alertarea administratorului atunci când sunt copiate informații pe dispozitive externe de stocare date. Pentru situații în care stația de lucru este offline, soluția va stoca informația respectivă local, iar la prima conectare on-line, va asigura alertarea administratorului.*	

					- *soluția trebuie să permită filtrarea fișierelor ce sunt copiate pe dispozitive externe de stocare date după extensie și /sau tip de fișier. Tipul de fișier trebuie identificat indiferent de extensia acestuia. (ex: blocarea copierii fișierelor Microsoft Office Word, Adobe Reader PDF).* - *soluția trebuie să nu poată fi oprită (stopată activitatea) de utilizator chiar dacă acesta are dreptul de administrator local.* - *soluția trebuie sa permita creare unei reguli de shadowing(duplicare) a fisierelor copiate pe dispozitive externe atunci cand anumite criteria sunt indeplinite (Ex: un anumit utilizator, grup de utilizatori, tipul fisierului, extensia fisierului). Duplicatul fisierului trebuie sa poata fi accesat numai de cei ce au acest drept in consola de administrare.* *<u>Protecția resurselor de rețea:</u>* - *să poată efectua descoperirea, indexarea și înregistrarea datelor din baze de date de tipul MySQL, Oracle.* - *pentru fișierele ce trebuiesc protejate să poată preveni upload-ul efectuat direct din consolă.* - *poluția trebuie asigure accesul la interfața de administrare prin intermediul unui portal web securizat SSL.* - *să permită aplicarea de filtre în procesul de descoperire a datelor (spre exemplu, excluderea fișierelor mai mari de X MB).* - *să poată efectua extragerea de informații din arhive cu peste 10 niveluri.* - *să permită setarea nivelului de resurse pe care în consumă (ex. lățimea de bandă la scanare).* - *soluția trebuie să scaneze incremental în CIFS, NFS, FTP.* *<u>Protecție Proxy:</u> soluția trebuie să fie capabilă să se integreze cu serviciul de proxy al BNM (McAfee WebGateway) și trebuie să protejeze împotriva transmiterii neautorizate de date şi informații prin protocoalele de rețea HTTP , HTTP/S şi FTP.* *<u>Protecție Email:</u> soluția trebuie să fie capabilă să se integreze cu serviciul de email al BNM (Microsoft Exchange 2013/2016, Outlook 2016).* *<u>Network monitor:</u>* - *soluția trebuie să fie capabilă să scaneze, analizeze și să clasifice în timp real traficul de ieșire din/în rețeaua Internet/BNM pentru majoritatea protocoalelor de rețea (HTTP, SMTP, IMAP, POP3, FTP,Telnet, Rlogin, SSH, webmail, Yahoo! Chat, AOL Chat, MSN Chat, ICY, TSP, SOCKS, PCAnywhere, RDP, VNC, SMB, Citrix, Skype, IRC, LDAP, DASL, NTLM, Kazaa, BitTorrent, eDonkey, Gnutella, DirectConnect, MP2P, WinMX, Sherlock, eMule, and more);* - *soluția trebuie să fie capabilă să se integreze pasiv cu echipamentul de rețea utilizând SPAN port sau "physically inline network tap" (optional);* - *soluția trebuie să asigure vizualizarea rapoartelor de incident.* ***<u>Cerințe privind administrarea:</u>***	

					- *consola trebuie să permită atribuirea automată a politicilor pe stații și servere în funcție de specificațiile sistemului. (Ex: Platforma desktop/server, Subnet, tip procesor, sistem de operare).* - *sincronizarea dintre server și client trebuie să se facă dinspre client către server.* - *administrarea componentelor de data loss prevention și de control al dispozitivelor externe trebuie să se poată face dintr-o singura consola.* - *consola de administrare trebuie să poată fi instalată într-un mediu virtual.* - *soluția trebuie să poată filtra evenimentele ce sunt generate de componentele aflate pe stațiile de lucru astfel încât baza de date sa nu se încarce cu informații considerate inutile.* - *soluția trebuie să permită configurarea de mesaje în funcție de tipul evenimentului.* - *accestul în consola de administrare să poată fi făcut pe baza credențialelor din Directory Services.* - *consola de administrare trebuie să permită creare de roluri în mod granular pentru cei ce o administrează.* - *soluția trebuie să ducă loguri (înregistrări de audit) cu privire la acțiunile utilizatorilor în consolă.* - *consola trebuie să permită construirea unei liste de contacte în vederea folosirii acestora pentru notificări prin mesagerie electronică (E-mail).* - *consola de administrare trebuie să poată fi accesată de pe orice computer din rețea în mod securizat, fără necesitatea instalării de software adițional.* - *daca serverul de administrare este accesat prin intermediul unei interfețe web, trebuie să fie posibil importul unui certificat ssl generat de o autoritate locala, înlocuindu-l astfel pe cel auto-generat.* - *sistemul trebuie să permită setarea periodicității de sincronizare dintre server și componente.* - *sistemul trebuie să permită setarea periodicității de transmitere a evenimentelor de pe client pe server.* - *sistemul trebuie să poată / permită automatizarea de sarcini de instalare / dezinstalare a componentelor pe stațiile de lucru, de rulare a rapoartelor și de transmiterea de notificări de prin mesagerie electronică.* - *sistemul (serverul) trebuie să fie capabil să declanșeze acțiuni automate atunci când anumite condiții sunt îndeplinite (ex: generarea unui eveniment pe server, pe o stație de lucru, detectarea unui nou sistem pe rețea).* - *soluția trebuie să permită aplicarea de politici diferite pentru sisteme pe: a. sisteme individuale; b. grupuri de sisteme; c. sisteme din Directory Services ce aparțin aceleiași OU.* - *soluția trebuie să permită accesarea logurilor componentei de sincronizare de pe sisteme în timp real prin intermediul unui serviciu web.* ***<u>Cerințe privind subsistemul de raportare:</u>*** - *soluția trebuie să asigure generarea de rapoarte despre nodurile administrate (endpoint-uri sau de rețea) și despre evenimentele generate de ele.*	

					- *soluția trebuie să permită crearea de noi rapoarte în mod granular cu informații extrase din evenimente, sau despre sistemele administrate.* - *rapoartele pot fi generate sub formă de tabel, pie chart, buble chart, listă, sumar, sau grafic istoric.* - *soluția trebuie să poată exporta rapoartele în cel puțin următoarele formate: pdf, csv, html.* - *soluția trebuie să permită personalizarea rapoartelor (ex. aplicarea logo-ului BNM).* - *soluția trebuie să permită atât salvarea sub formă de fișiere a rapoartelor cât și expedierea acestora prin e-mail.* - *soluția trebuie să permită aplicarea de filtre pe evenimente la generarea rapoartelor.* - *soluția trebuie să poată genera rapoarte privind (dar nelimitându-se la):* ✓ *log-urile de audit administrative;* ✓ *detalii despre sistemele administrate (detalii de configurare, hardware, utilizator);* ✓ *evenimente de la sistem;* ✓ *Informații despre politicile și sarcinile aplicate sistemelor;* ✓ *Informații furnizate de agenți.* ***Alte cerințe obligatorii:*** *Perioada de suport standard de la producător trebuie să fie egalată cu perioada licențelor DLP exploatate în cadrul Sistemului Informațional al BNM, până la 13.12.2020* ***Termen de livrare:*** *până la 13.12.2019 inclusiv.*	
2	72268000-1	Servicii de asigurare a accesului la suport anual Business Support, sau echivalentul, pentru licența McAfee Total Protection for Data Loss Prevention Software pentru 350 utilizatori	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 14.12.2019-13.12.2020 pentru licențele McAfee Total Protection for Data Loss Prevention Software exploatate în cadrul Sistemului Informațional al BNM pentru 350 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: *până la 13.12.2019 inclusiv*	
3	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 anuală pentru perioada 07.11.2019 - 06.11.2020 a licenței McAfee Web Protection exploatată în cadrul Sistemului Informațional al BNM, cu un an de suport de tipul Business Support inclus, sau echivalentul, cu extinderea până la 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:*** *până la 07.11.2019 inclusiv*	
Lotul 3: Menținerea soluției IBM Qradar						196 666,67
1	72268000-1	Servicii de asigurare a accesului la menținerea anuală a instrumentului IBM Security Qradar	buc	1	**Tip:** *Servicii de asigurare a accesului la suport anual de la producătorul licențelor de tip Annual Software Subscription & Support Renewal 12 Months, sau echivalentul, pentru perioada 01.11.2019 - 31.10.2020, 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 până la 01.11.2019 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*	
2	72268000-1	Servicii de asigurare a accesului la menținerea anuală a modulului IBM Security QRadar Vulnerability Manager	buc	1	**Tip:** *Servicii de asigurare a accesului la suport anual de la producătorul licențelor de tip Annual Software Subscription & Support Renewal 12 Months, sau echivalentul, pentru perioada 01.01.2020 - 31.12.2020 a modulului IBM Security QRadar Vulnerability Manager, 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 până la 26.12.2019 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 de gestionare a accesului privilegiat la resursele Sistemului Informațional al BNM prin protocoalele RDP și SSH***						592 500,00
	48730000-4	Soluție de gestionare a accesului privilegiat la resursele Sistemului Informațional al BNM prin protocoalele RDP și SSH, inclusiv 12 luni de suport local și menținere de la producător	buc	1	*<u>Tip:</u> Soluție de gestionare a accesului privilegiat la SI al BNM prin protocoalele RDP și SSH (Privileged Access Management - PAM). Soluția oferită trebuie să efectueze controlul securității informațiilor pentru utilizatorii din afara sistemului, ce oferă suport la distanță conform contractelor de mentenanță, încheiate cu BNM, ce va permite gestionarea accesului privilegiat la infrastructura existent.* *<u>Cantitatea:</u> Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul numărul de sisteme - 50 de sisteme și că numărul de sesiuni concurente/utilizatori către aceste 50 de sisteme (Windows, Linux, Aplicații) fiind nelimitat.* ***<u>Cerințe funcționale şi tehnice:</u>*** *· Soluția trebuie să fie propusă ca un Appliance Virtual compatibilă cu mediul virtual Vmware sau Citrix.* *· Soluția trebuie să suporte cel puțin următoarele protocoale:* *o RDP, SSH pentru conexiunile dintre utilizator şi soluție* *o SSH, SCP, RDP,VNC, TELNET pentru conexiunile dintre soluție şi sistemele organizației* *o Aplicațiile de tip thickclient trebuie să poată fi accesate prin intermediul serverelor de tip Jump off, prin RDP RemoteApp mode.* *· Pentru conexiunile între PAM şi sistemele organizației trebuie să fie posibil de configurat drepturi granulare ce țin de funcționalul protocoalelor utilizate (de exemplu, permiterea sesiunii RDP, dar interzicerea copierii fişierelor prin intermediul copy/paste în cadrul sesiunii RDP, etc.).* *· Soluția sa fie uşor de extins la cererea Cumpărătorului (licențe, noduri, spațiu).* *· Soluția trebuie să asigure securitatea (integritatea, confidențialitatea şi disponibilitatea) informațiilor stocate, inclusiv a jurnalelor de evidență şi a înregistrărilor sesiunilor PAM.* *· Soluția trebuie să ofere managementul centralizat al tuturor componentelor și funcțiilor administrative dintr-o singură interfață de utilizator, bazată pe o interfață web.* *· Soluția trebuie să aibă o consolă de administrare cu un conținut "User Friendly" și intuitivă pentru administrarea sistemului.* *· Administratorul trebuie să poată defini granular rolurile de acces la sistem, specificând funcții, modalitatea de raportare. Trebuie să fie posibilă limitarea drepturilor pentru rolul de administrator al soluției de a accesa sistemele informatice integrate în soluție.* *· Soluția trebuie să suporte o interfață grafică, pagină web pentru gestionare, analiză și raportare.* *· Soluția trebuie să posede sisteme (task-uri) automate de backup/recovery.*	

					· Soluția trebuie să permită implementarea unui flux de aprobare a solicitărilor de acces prin PAM la sistemele informatice, precum şi de vizualizare a credențialelor pentru conturile de administrator, stocate în PAM. *· Soluția trebuie să ofere mecanisme de notificare în timp real prin email pentru o imediată răspundere la solicitările de acces sau vizualizare a credențialelor stocate în PAM.* *· Soluția trebuie sa fie integrabilă cu soluțiile SIEM/SYSLog.* *· Soluția trebuie să aibă capacitatea automată de a descoperi drepturile privilegiate a utilizatorilor pentru înscrierea ulterioară a acestora în PAM.* *· Soluția trebuie să aibă suport de înaltă disponibilitate (HA) și instanță DR cu replicare în timp real.* *· Soluția trebuie să suporte arhivarea manuală şi automată prin copierea înregistrărilor video şi a evenimentelor pe diferite soluții de stocare NFS, CIFS.* *· Soluția trebuie să suporte arhivarea/comprimarea logurilor.* *· Controlul accesului la conturile partajate, va permite utilizatorilor autorizați să le acceseze în urma unui flux de aprobare de către persoanele responsabile sau deținătorii de sisteme.* *· Credențialele trebuie să fie protejate împotriva compromiterii din partea utilizatorilor.* *· Istoricul tuturor aprobărilor de acces sau vizualizare de credențiale trebuie să fie păstrat pe un termen nelimitat și cu asigurarea integrității.* *· Păstrarea unei căi de audit care stochează toate utilizările conturilor utilizatorilor privilegiați.* *· Soluția trebuie să susțină controlul sesiunilor, înregistrarea lor (pentru analiza ulterioară) și monitorizarea în timp real a sesiunilor pentru a urmări activitatea utilizatorilor și pentru a detecta evenimentele suspecte.* *· Soluția trebuie să înregistreze toate procesele pornite şi stopate pe sistemele Windows de către administratorii de sisteme.* *· Soluția trebuie să furnizeze o arhitectură bazată pe proxy sau în unele cazuri o arhitectură Jump Server care să ofere un singur punct de control al accesului și să impună monitorizarea și înregistrarea tuturor activităților privilegiate.* *· Soluția trebuie să permită încetarea imediată a sesiunile privilegiate suspecte direct din consola administrativă.* *· Soluția trebuie să furnizeze jurnale de auditare a sesiunilor și înregistrări video care să permită definirea momentului în care s-a început un incident, să înțeleagă cum a început incidentul și să evalueze rapid orice prejudiciu.* *· Soluția trebuie să aibă o bază de date pentru stocarea înregistrărilor de sesiuni și a jurnalelor de audit pentru a împiedica utilizatorii să își editeze istoricul activităților.* *· Soluția va putea vizualiza și monitoriza cu ușurință toate sesiunile de aplicații, RDP și SSH. Managerul de sesiuni trebuie, de asemenea, să avertizeze echipele de securitate cu privire la activitatea suspectă și să înceteze sesiunile de la distanță.* *· Soluția trebuie să limiteze (filtreze) comenzile care pot fi executate sub modul privilegiat.*	

					· *Soluția trebuie să ofere acces de control predefinite pe perioade specificate de timp, dată, locație de acces.* · *Soluția trebuie să înregistreze toate execuțiile comenzilor privilegiate SSH.* · *Soluția trebuie să se integreze cu sisteme de autentificare multi-factor.* · *Soluția trebuie sa permită citirea grupelor din AD/LDAP şi înscrierea lor in grupul local PAM.* · *Soluția trebuie să ofere posibilitatea de autentificare pe sisteme prin următoarele metode:* o *Interactive - utilizatorul PAM trebuie să introducă manual credențialele (fără stocarea acestora în PAM).* o *Mapare - PAM autentifică utilizatorul pe sistem utilizînd credențialele utilizate pentru autentificare pe PAM.* o *Vault - PAM autentifică utilizatorul pe sistem utilizînd credențialele stocate securizat în soluția PAM.* · *Soluția trebuie să ofere API pentru funcționalul de bază al acesteia care să permită integrarea soluției cu alte sisteme de securitate precum IAM, SIEM, etc.* · *Modelul de licențiere trebuie să permită conectarea de sisteme suplimentare (scalabilitate), cu achiziționarea licenței respective. Totodată, trebuie să fie posibilă modificarea modelului de licențiere (per număr de sisteme la per număr de sesiuni concurente şi viceversa), în momente de timp binedefinite.* · *Tipul licenței - Perpetual* <u>*Cerințe suplimentare:*</u> *Soluția trebuie să dețină posibilitatea ulterior de a fi extinsă pentru următoarele capabilități:* · *Soluția trebuie să poată gestiona securizat credențialele pentru conturile de tip a2a sau s2s (aplicație/sistem către aplicație/sistem). Aplicațiile trebuie să se conecteze securizat şi automatizat prin intermediul API către PAM şi să extragă parolele pentru conturile utilizate pentru conexiuni către alte aplicații sau baze de date, fără interacțiune umană.* · *Soluția trebuie să ofere un mecanism sigur de recuperare a credențialelor în caz de indisponibilitate completă a soluției.* · *Parolele pentru conturile de administrare și cele partajate trebuie să fie gestionate în conformitate cu politicile definite.* · *Funcțiile de reconciliere trebuie să verifice dacă parolele nu au fost modificate prin niciun alt mecanism, iar istoricul parolei va fi disponibil pentru a sprijini restabilirea copiilor de rezervă anterioare.* · *Soluția trebuie să permită securizarea, gestionarea și urmărirea utilizării credențialelor privilegiate, între sisteme de operare, baze de date, aplicații, etc.* · *Soluția trebuie să asigure aplicarea automată a politicilor de parole pentru conturilor privilegiate, cu flexibilitatea de aplicare cu ușurință politicile granulare pentru anumite cerințe de conformitate sau cerințe privind unitățile comerciale. Soluția trebuie să securizeze*	

					parolele și cheile SSH într-un seif certificat (algoritmul de criptare AES 256) și să utilizeze arhitectura deschisă pentru a se integra cu alte seifuri. *· Soluția trebuie să programeze rotirea și revocarea parolelor și SSH cheilor, utilizând un nivel înalt, granular de management ce permite impunerea politicilor de securitate prin intermediul unor fluxuri de lucru personalizabile.* *· Pentru cazuri de urgență, soluția trebuie să ofere mecanisme de vizualizare a parolelor (cu flux de aprobare) de către utilizatori pentru o anumită perioadă, cu schimbarea automată a acestor parole după expirarea perioadei menționate.* *· Gestionarea parolelor și altor credențiale pentru aplicațiile Web și ThinkClient (Oracle, etc.).* *<u>Perioada de suport local și menținere de la producător</u>:* *1. Pentru soluția ofertată se solicită a fi 12 luni* *2. Producătorul trebuie să ofere suport prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului.* *3. Suportul solicitat este de 8/5 (opt ore /cinci zile) conform orarului de lucru a Beneficiarului.* *<u>Notă:</u>* *Pentru verificarea corespunderii cerințelor înaintate, după deschiderea ofertelor, la solicitarea autorității contractante în decurs de 3 zile lucrătoare Ofertantul va oferi versiunea trial a soluției ofertate pentru testare.* *Lucrările de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției și asigurarea suportului la definirea/configurarea și exploatarea soluției pentru primul an de exploatare precum și transferul de cunoștințe Beneficiarului inclusiv furnizarea documentației de instalare, configurare și restabilire a serviciului oferit, trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă. De asemenea Ofertantul trebuie să integreze în soluția PAM următoarele tipuri de sisteme:* *· Windows – 4 sisteme* *· Linux – 4 sisteme* *· Aplicații web (HTTP) – 1 unitate* *· Aplicații specific (SQL Studio) – 1 unitate* *Ofertantul trebuie să ofere instrucțiuni privind integrarea acestor tipuri de sisteme în soluția PAM.* ***Termen de livrare:** 30 zile lucrătoare de la data intrării în vigoare a contractului, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.*	
Valoarea estimată totală, MDL, fără TVA:						**1 429 166,67**

8. Admiterea sau interzicerea ofertelor alternative: nu se admite.

9. **Termenii și condițiile de livrare solicitați: C*onform limitei/perioadei indicate în formularul F4.2 (Specificații de preț). Vânzătorul va asigura livrarea bunurilor în corespundere cu toate cerințele înaintate.***

10. Contract de achiziție rezervat atelierelor protejate sau că acesta poate fi executat numai în cadrul unor programe de angajare protejată (după caz): Nu.

11. Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora și a criteriilor de selecție; nivelul minim (nivelurile minime) al (ale) cerințelor eventual impuse; se menționează informațiile solicitate (DUAE, documentație):

Nr. d/o	Descrierea criteriului/cerinței	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativitatea
1	Formularul ofertei	*Original- conform formularului F3.1, confirmat prin ștampila și semnătura participantului*	DA
2	Specificații tehnice	*Original- conform formularului F4.1, confirmat prin ștampila și semnătura participantului*	DA
3	Specificații de preț	*Original- conform formularului F4.2, confirmat prin ștampila și semnătura participantului*	DA
4	Formularul DUAE	*Original- confirmat prin ștampila și semnătura participantului*	DA
5	Garanția pentru ofertă	**Forma garanției:** *a) Oferta va fi însoțită de o Garanție pentru ofertă (emisă de o bancă comercială) conform formularului F3.2 din secțiunea a 3-a – Formulare pentru depunerea ofertei din documentația standard* sau *b) Garanția pentru ofertă prin transfer la contul autorității contractante, conform următoarelor date bancare:* *Beneficiarul plății: Banca Națională a Moldovei* *Denumirea Băncii: Banca Națională a Moldovei* *Codul fiscal: 79592* *IBAN: MD12NB000000000004914852* *Contul bancar: NBMDMD2X* *cu nota "Pentru garanția pentru ofertă la licitația publică nr.____ din _____"* **Cerințe față de garanție:** Garanția pentru ofertă va fi în valoare de: *1% din valoarea ofertei fără TVA.*	DA

6	Garanția de bună execuție (la încheierea contractului atribuit)	*Garanția de buna execuție (emisă de o bancă comercială) conform formularului F3.3 Termenul de valabilitate a garanției va fi egal cu termenul de valabilitate a contractului.* *sau* *b)Garanția de bună execuție prin transfer la contul autorității contractante, conform următoarelor date bancare:* *Beneficiarul plății: Banca Națională a Moldovei* *Denumirea Băncii: Banca Națională a Moldovei* *Codul fiscal: 79592* *IBAN: MD65NB000000000004914771* *Contul bancar: NBMDMD2X* *cu nota "Pentru garanția de bună executare a contractului atribuit prin procedura de licitație deschisă nr._____ din _____"* ***Cerințe față de garanție:*** *Garanția de bună execuție (se stabileşte procentual din prețul contractului adjudecat): 5%.*	
7	Măsuri de identificare a clientului, de monitorizare a activităților şi tranzacțiilor, conform procedurilor interne ale Băncii Naționale a Moldovei cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.	*Chestionar pentru Furnizor F3.5 – original / copie - confirmat prin aplicarea ștampilei și semnăturii participantului* *(Se va prezenta în mod obligatoriu la încheierea contractului de achiziție de către Ofertantul desemnat câștigător)*	NU
8	Raport financiar	*Copia ultimului raport financiar pentru anul 2018 confirmat prin aplicarea semnăturii și ștampilei participantului.*	DA
9	Dovada înregistrării persoanei juridice	*Certificat/decizie de înregistrare a întreprinderii sau extras, care certifică statutul de persoană juridică a Ofertantului – copie conform cu originalul – emis de Camera Înregistrării de Stat / I.P.„Agenția Servicii Publice"*	DA
10	Certificat de atribuire a contului bancar	*Copie conform cu originalul (confirmat prin aplicarea semnăturii și ștampilei ofertantului)– eliberat de banca deținătoare de cont după data punerii în aplicare a codurilor IBAN*	DA

11	Demonstrarea experienței operatorului economic în domeniul de activitate aferent obiectului contractului ce urmează a fi atribuit	*Ofertantul trebuie să posede o experiență specifică în prestarea serviciilor și/sau livrarea bunurilor similare de cel puțin 1 an în domeniu, reputație bună, să fie dotat cu tehnică necesară şi să dispună de competențe profesionale, echipament şi alte resurse, inclusiv servicii post-vânzare, precum şi competențe manageriale, experiență specifică, personal calificat necesar pentru realizarea contractului şi alte capacități necesare pentru a executa contractul de achiziție publică la calitatea solicitată, pe toată perioada de valabilitate.* *Pentru demonstrarea îndeplinirii acestor cerințe operatorul economic completează "Declarația privind lista principalelor prestări servicii și/sau livrări de bunuri similare în ultimii ani", iar în scopul verificării și confirmării informațiilor declarate, ofertantul trebuie să fie dispus să prezinte la solicitare următoarele documente suport:* *- copie (extras) ale respectivului/ respectivelor contract/ contracte, astfel încât autoritatea contractantă să poată identifica natura bunurilor livrate/serviciilor prestate, valoarea acestora și prețul,* *și/sau* *- scrisori de recomandare din partea beneficiarilor/clienților.*	DA
12	Actul care atestă dreptul de livrare a bunurilor/prestare a serviciilor	*Copia certificatului ce atestă relația Ofertantului cu Producătorul sau copia certificatului de partener autorizat al producătorului sau autorizației de livrare.* *Suplimentar pentru Lotul 4, Ofertantul trebuie să prezinte Certificatul de la Producător ce atestă dreptul Ofertantului de a presta servicii de suport tehnic pentru soluția ofertată.*	DA
14	Demonstrarea accesului la personalul necesar pentru îndeplinirea corespunzătoare a obiectului contractului ce urmează a fi atribuit (personalul de specialitate care va avea un rol esențial în îndeplinirea acestuia)	*Cerințe suplimentare pentru lotul 1, 4:* *- Ofertantul trebuie să aibă cel puțin o referință de instalare pentru soluția propusă.* *- Ofertantul trebuie să prezinte dovezi că poate pune la dispoziția Beneficiarului pentru executarea contractului de achiziție publică specialiști calificați certificați de către Producătorul soluției care vor fi responsabili pentru instalarea/configurarea soluției ofertate în conformitate cu cerințele stabilite de Beneficiar (să fie anexate certificatele corespunzătoare).*	DA

12. **Criteriul de evaluare aplicat pentru adjudecarea contractului: *<u>Prețul cel mai scăzut, fără TVA, pe loturi</u>, cu corespunderea cerințelor față de ofertant şi corespunderea cerințelor tehnice minime obligatorii privind obiectul achiziției.***

13. **Termenul limită de depunere/deschidere a ofertelor:**

1. până la: *ora*_____
2. pe data de: _____

14. Adresa la care trebuie transmise ofertele sau cererile de participare:

    Ofertele vor fi depuse electronic pentru fiecare lot în parte prin intermediul SIA RSAP „M-Tender”.

15. Termenul de valabilitate a ofertelor: 60 zile calendaristice.

    Notă: În oferta participanților va fi indicat explicit termenul de valabilitate a ei.

16. Locul deschiderii ofertelor: SIA RSAP „M-Tender”.

    Ofertele întârziate vor fi respinse.

17. Limba sau limbile în care trebuie redactate ofertele: limba română.
18. Alte informații relevante:
    a. *Facturile fiscale urmează a fi emise de către furnizorii rezidenți, sau în mod electronic prin SIA e-Factura sau dacă nu e posibil pe suport de hârtie*

19. Denumirea și adresa organismului competent de soluționare a contestațiilor:
    Agenția Națională pentru Soluționarea Contestațiilor
    Adresa: mun. Chișinău, bd. Ștefan cel Mare și Sfânt nr.124 (et.4), MD 2001;
    Tel/Fax/email: 022-820 652, 022 820-651, contestatii@ansc.md
20. Data transmiterii spre publicare a anunțului de participare: _____

Conducătorul grupului de lucru: Ion STURZU _____ L.Ș