**Î.S. „Posta Moldovei”**
*IDNO 1002600023242, bd. Ştefan cel mare şi Sfânt, nr 134, mun. Chişinău, RM*

**ANEXA NR.1**

**SPECIFICAŢIA TEHNICĂ**

**Expunerea obiectului de achiziţie – Pachete software antivirus**

## Capitolul I – Date generale cu privire la entitatea contractantă

**1.** Denumirea entității contractante: **Î.S. „Poșta Moldovei”**

**2.** IDNO: **1002600023242**

**3.** Adresa: **Municipiul Chișinău, bd. Ștefan Cel Mare și Sfânt, nr. 134, RM**

**4.** Numărul de telefon oficial al entității contractante: **+373 (61) 251-233**

**5.** Adresa de e-mail oficială a entității contractante: **cancelaria@poșta.md**

**6.** Pagina web oficială a entității contractante: **www.posta.md**

**7.** Tipul entității contractante și obiectul principal de activitate:

- **Întreprindere de stat la autogestiune, servicii poștale și financiare;**
- **Activitățile sectoriale în domeniul serviciilor poștale.**

**8.** Date de contact în cadrul procedurii de achiziție:

- Nume: **Victor IVANOV**
- Nr. de contact: **+373 (61) 119-154**
- Adresa de e-mail: **victor.ivanov@posta.md, grup.achizitii@posta.md.**

## Capitolul II – Date generale cu privire la procedura de achiziție

**1. Procedura de achiziție este realizată sub incidența actului normativ:** Legea privind achizițiile în sectoarele energeticii, apei, transporturilor și serviciilor poștale 74/2020;

**2. Obiectul achiziției:** Materiale de construcție;

**3. Valoarea estimată:** 833 333,33 lei *(fără TVA);*

**4. Cod CPV:** 48200000-0;

**5. Criteriu de evaluare aplicat**: cel mai mic preț;

**6. Procedura de achiziție sectorială aplicată**: Licitație deschisă;

**7. Condiții de achitare**: în termen de 30 zile din data semnării facturilor fiscale.

## Capitolul III – Alte informații relevante:

**1.** Entitatea contractantă va utiliza *(după caz)* motivele de excludere prevăzute la art. 19 din Legea nr. 131/2015 privind achizițiile publice;

**2.** Oferta va fi întocmită clar, fără corectări, în limba română, cu semnătura electronică a Ofertantului sau a persoanei împuternicite. În cazul în care oferta este semnată și depusă de o persoană împuternicită, ofertantul va prezenta și procura sau alt document care confirmă această împuternicire;

**3.** Completarea defectuoasă a formularelor anexate în cadrul procedurii de achiziție poate fi considerată ca neîndeplinirea criteriilor de calificare și selecție și respectiv va atrage respingerea ofertei ca fiind necorespunzătoare;

**4.** Cerințele specificate sunt minime și obligatorii. În acest sens, orice ofertă care prezintă bunuri cu caracteristici tehnice inferioare celor prevăzute sau care nu satisfac cerințele minime indicate, va fi respinsă ca neconformă;

**5.** Specificația tehnică *(anexa nr. 1)* face parte integrantă din documentația de atribuire și constituie ansamblul cerințelor minime pe baza cărora ofertantul va elabora oferta pentru prestarea serviciilor menționate;

## Capitolul IV – Specificaţia tehnică:

**Tip:** Subscriere anuală pentru soluţia de protecţie şi securitate pentru 1000 entităţi (PC/ laptop/ VDI/ Server) pentru perioada de 3 ani.

**Cantitate:** Ofertantului este responsabil de a determinarea modelului de licenţiere luând în calcul:

- 1000 entităţi *(PC/laptop/VDI/Server);*
- Disk Encryption management pentru 1000 entităţi.

Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaţionale independente cu renume mondial în domeniu *(certificări "AV-TEST", "VIRUS BULLETIN'S", "REAL-WORLD PROTECTION", "MALWARE PROTECTION").*

### *Caracteristici generale ale produsului:*

Soluţia trebuie să reprezinte o platformă integrată pentru managementul securităţii, gândită ca o soluţie modulară.

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

- Protecţie staţii şi servere fizice şi virtualizate;
- Serviciu de corelare şi răspuns la evenimente de tip EDR *(endpoint detection and response).*

### *Consola de management:*

Accesibilitate atât de pe browser desktop cât şi tip mobile.

Să ofere opţiune configurabilă de actualizare automată a consolei de management.

### *Soluţia de scanare centralizată:*

Soluţia trebuie să asigure protecţia mediilor virtualizate *(VDI)*, inclusiv a mediilor persistente şi non-persistente, şi să fie compatibilă cu următoarele platforme de virtualizare:

**1.** VMware vSphere;
**2.** Citrix XenServer;
**3.** Microsoft Hyper-V.

### *Cerinţe generale produs:*

Soluţia trebuie să:

- permită activarea/dezactivarea actualizărilor automate de produs/semnături şi a consolei de management;
- ofere vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcţii noi si îmbunătăţiri, probleme rezolvate, probleme cunoscute;
- afişeze notificările şi alertele existente, să alerteze administratorul în cazul unor probleme majore *(configurabile)*: licenţiere, detecţie viruşi, actualizări de produs disponibile.

### *Panou de monitorizare si raportare (Dashboard):*

- să ofere posibilitatea creării rapoartelor configurabile după tip, ţintă şi scop cu opţiuni specifice pentru orice tip de raport cu posibilităţi de adăugare/eliminare şi rearanjare.
- să prezinte rapoarte pentru toate modulele suportate *(stare/statut/actualizare)*.

### *Inventarierea reţelei – managementul securităţii:*

Produsul trebuie să:

- se integreze cu domenii Active Directory multiple, să poată importa inventarul.
- permită descoperirea PC neintegrate în Active Directory (Workgroup);
- ofere opţiuni de căutare, sortare şi filtrare după numele sistemului, sistem de operare si adresa IP, politica aplicată, online şi/sau offline şi FQDN;
- permită instalarea la distanţă sau manual a clienţilor antivirus pe maşini fizice şi virtuale;
- permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe maşinile fizice/virtuale;
- permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanţă pentru clientul antivirus;
- ofere posibilitatea de repornire a maşinilor fizice de la distanţă;
- ofere informaţii detaliate despre fiecare task iniţiat şi afişarea statutului lui;
- permită configurarea centralizată a clienţilor antivirus prin intermediul politicilor;
- ofere în consola de management informaţii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături;
- permită descoperirea tuturor aplicaţiilor instalate pe toate staţiile şi serverele din reţea.

## ***Politici:***

Produsul trebuie să:

- permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conţine setări pentru toate module;
- conţină opţiuni specifice de activare/dezactivare şi configurare a funcţionalităţilor precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicaţiilor, scanarea traficului web, controlul dispozitivelor, power user;
- permită aplicarea politicilor pe maşini client, grupuri de maşini, pool-uri de resurse (VMware), domeniu, unităţi organizaţionale sau useri de active directoy;
- poată fi schimbată automat în funcţie de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este în accesai reţea cu infrastructura de management, Tipul reţelei (lan, wireless).

## ***Monitorizare şi raportare:***

Produsul trebuie să:

- permită setarea de opţiuni specifice pentru afişarea rapoartelor existente;
- deţină un panou central care să afişeze statutul modulelor şi rapoartele lor pentru perioadele de timp specificate;
- conţină rapoarte care prezinta statutul maşinilor clienţilor, al actualizărilor, fişierelor malware detectate, aplicaţiile 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, menţinând informaţiile concise si ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal;
- ofere interogări legate de starea terminalului precum: tip maşină, infrastructură reţelei căreia aparţine, datele agentului de securitate, starea modulelor de protecţie, rolurile terminalelor;
- ofere interogări legate de evenimente precum: calculatorul ţinta pe care a avut loc evenimentul, tipul starea şi configuraţia agentului de securitate instalat, starea modulelor şi rolurilor de protecţie instalate pe agentul de securitate, denumirea şi alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicaţii blocate, detecţiile etc);

## ***Carantină:***

- Produsul trebuie să permită restaurarea fişierelor din carantină în locaţia originală sau într-o cale configurabilă;
- Administrarea Carantinei să fie posibilă atât pe terminalul administrat cât şi din consola de management;

## ***Utilizatori:***

- Administrarea este necesar să fie efectuată pe bază de roluri multiple predefinite: Administrator companie, Administrator reţea, Reporter şi alte roluri configurabile detaliat cu posibilitatea de selectare a serviciilor şi obiectelor pentru care un utilizator poate face modificări;
- Utilizatorii să poată fi importaţi din Microsoft Active Directory sau creaţi în consola de management;
- Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp - configurabil.

## ***Log-uri:***

- Soluţia trebuie să permită înregistrarea acţiunilor utilizatorilor şi să ofere informaţii detaliate pentru fiecare acţiune a unui utilizator cu posibilitatea de filtrare.

## ***Actualizare:***

Soluţia va permite:

- Definirea de locaţii de actualizare multiple;
- Activarea/dezactivarea actualizărilor;
- Testarea noilor versiuni înainte de a fi instalate pe toţi clienţii *(posibilitate de actualizare în mai multe cicluri – 1 mediu de test, 2 – mediu de producţie);*
- Definirea zonelor de test şi zonelor critice de producţie.

## ***Protecţie staţii şi servere fizice si virtualizate – caracteristici minime:***

Soluţia trebuie să:

- Permită instalarea personalizată a modulelor;
- Includă un „vaccin" anti-ransomware, cu actualizări de la producător, pentru protecţia împotriva tuturor ameninţărilor cunoscute de tip ransomware, prin imunizarea staţiilor şi serverelor, chiar daca sunt infectate şi blocarea procesului de criptare;
- Includă protecţie împotriva atacurilor zero-day de tip exploit *(atacuri direcţionate);*
- Includă modul de analiză la risc capabil să identifice şi să remedieze riscurile identificate la nivel de reţea sau sistem de operare, cu posibilitate de configurare şi automatizare;
- Includă un modul avansat de securitate bazat pe tehnologii de machine learning, analiză comportamentală şi algoritmi euristici, proiectat pentru detectarea atacurilor avansate şi a activităţilor suspecte înainte de faza de execuţie;
- Includă modul avansat de securitate pentru protecţie împotriva: atacurilor direcţionate *(Targeted Attack),* fişierelor suspecte si traficului la nivel de reţea suspect, exploit-urilor, ransomware şi grayware. Fiecărui tip de ameninţare trebuie să i se poată configura independent nivelul de protecţie şi acţiunile aplicate, în funcţie de capabilităţile soluţiei ofertate şi recomandările producătorului;
- Includă modul de sandbox, unde se vor putea trimite manual sau automat fişiere pentru a putea fi „detonate" pentru o analiză în profunzime;

• Includă variante de analiză a sandbox-ului tip: doar monitorizare sau blocare cu acţiuni de remediere: implicită şi de siguranţa. Pentru acţiunea implicită: doar raportare, dezinfecţie, ştergere şi transmitere în carantină. Pentru acţiunea de siguranţa: ştergere sau permutare în carantină;

• Suporte "detonarea" în modulul sandbox, minim, tipurile de fişiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML *(Unicode)*, JAR *(archive),* JS, LNK, MHTML *(doc),* MHTML *(ppt),* MHTML *(xls),* Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files *(executable),* PDF, PEF *(executable),* PIF *(executable),* RTF, SCR, URL *(binary),* VBE, VBS, WSF, WSH, WSH-VBS, XHTML. Acestea vor fi detectate corect chiar dacă vor fi în arhive de tipul : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP *(multivolume),* ZOO, XZ ;

• Ofere posibilitate de filtrare a incidentelor din interfaţa grafică în funcţie intervalul de timp, pe baza unui scor de încredere, indicatori de atac, tehnici de atac, sistem de operare afectat cît şi după IP, nume fişier, nume staţie;

• Permită vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod: să generează o hartă de principiu a incidentului, să detalieze incidentul în funcţie de amprenta de timp a fiecărei acţiuni aferente incidentului, să poată genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigare – virus total, sandbox, google – la nivel de fişier, adăugare în lista de blocare – la nivel de reţea sau instalare patch – la nivel de nod);

• Poată bloca fişiere şi/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fişier CSV;

• Poată excepta fişiere non-maliţioase de la acţiunea de investigare sau poate genera/adaugă un set de fişiere maliţioase într-o listă neagră pentru a preveni mişcarea laterală a fişierelor/proceselor maliţioase;

• Permită deschiderea unei conexiuni remote către un endpoint potenţial infectat pentru a permite o investigare rapidă a gazdei/ colectare date despre atacul respectiv/ remediere în timp real a breşelor de securitate/ permită executarea unor comenzi în linia de comandă care se execută cu privilegii de kernel pentru eliminarea în timp real a unor ameninţări sau colectarea de date privitoare la atacul în desfăşurare;

• Permită crearea regulilor de detecţie customizabilă bazată pe procese, fişiere, registre şi conexiuni de reţea;

• Permită creare regulilor de excludere customizabilă bazată pe procese, fişiere, registre si conexiuni de reţea;

• Permită căutarea pro activă pe endpoint-urile protejate a indicatorilor de compromitere precum hash-uri, nume de fişiere, nume de procese, chei de registre, valori de registre;

• Permită deschiderea unei conexiuni remote către un endpoint potenţial infectat pentru investigare rapidă, colectare date şi remedierea în timp real a breşei de securitate, reducând timpul de remediere (downtime) în cazul unui atac, executarea comenzilor în linia de comandă cu privilegii de kernel ce permit eliminarea în timp real a unor ameninţări sau colectarea de date privitoare la atacul în desfăşurare;

• Includă modul de detectare, corelare şi răspuns la evenimente de tip EDR („endpoint detection and response") capabil să identifice ameninţări avansate sau atacuri în curs de desfăşurare. Acest modul va fi capabil să:

***a)*** *cuprindă colectarea de date şi evenimente despre hardware şi software aferent fiecărei staţii de lucru aducând informaţii detaliate referitoare la incidentele detectate, o hartă detaliata a acestora precum şi acţiuni de remediere automate şi integrare cu modulele de Sandbox şi modulul avansat de securitate;*

***b)*** *ofere senzori de colectare a datelor şi componente de procesare şi interpretare a acestora;*

***c)*** *posede capacitărăți de evaluare a activității tipice a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining") și va raporta orice deviație de la acest comportament sub forma unui incident;*

***d)*** *ofere vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat generînd o hartă de principiu a incidentului, detaliind incidentul în funcție de amprenta de timp a fiecărei actiuni aferente incidentului, respectiv butonul „acționează" care poate genera un set de masuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod);*

***e)*** *poate bloca fișiere si/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV;*

***f)*** *poată excepta fișiere non-maliționase de la acțiunea de investigare sau poate genera/adaugă un set de fișiere maliționase într-o listă pentru a preveni mișcarea laterală a fișierelor/proceselor maliționase;*

***g)*** *permită vizualizarea incidentelor extinse corelate de pe mai multe endpoint-uri.*

## ***Cerințe de sistem:***

• Sisteme de operare pentru stații de lucru: Windows 7/10/11 (inclusiv Embebed și IoT), Mac OS X de la 10.12 și mai recent, Red Hat Enterprise Linux / CentOS 7 și mai recent, Oracle Linux 6.3 și mai recent, Ubuntu 16 și mai recent, SUSE Linux Enterprise Server 12 și mai recent, OpenSUSE 15 și mai recent, Fedora 31 și mai recent;

• Sisteme de operare Windows pentru servere: Windows Server 2012/2012 R2/2016/2019/2022.

## ***Administrare și instalare remote:***

• Pachetele de instalare trebuie să fie configurabile cu modulele necesare cu domenii tip firewall, device control, power user, content control, disk encryption, EDR sensor, „relay" *(update server");*

• Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management;

• Din consola să fie disponibile informații despre fiecare endpoint: numele, IP, sistem de operare, module instalate, politica aplicată, informații despre actualizări;

• Posibilități de creare kit pentru endpoint – tip: universar – 32/64bit, fizic/VDI, web installe/full;

• Gestionare, creare și configurare grupuri pentru endpoint ce nu sunt în AD;

• Posibilitate de atribuire a funcționalității de descoperire a endpointurilor și în afara AD, pentru oricare endpoint.

## ***Caracteristici și funcționalități principale ale modulului antivirus:***

Produsul trebuie sa permită:

• Stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni:

***a)*** *implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune;*

***b)*** *alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină;*

***c)*** *acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune;*

***d)*** *acţiune alternativă pentru fişierele suspecte: interzice accesul, ştergere, mută fişierele în carantină;*

• Scanarea automată în timp real cu setarea excepţiilor, definirea unor liste de excludere de la scanarea în timp real şi la cerere a anumitor directoare, discuri, fişiere, extensii sau procese, să nu scaneze arhive sau fişiere 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 aplicaţii cu potenţial periculos protejând sistemul de viruşii necunoscuţi prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă;

• Scanarea oricărui suport de stocare a informaţiei *(CD-uri, harduri externe, unităţi partajate etc);*

• Scanarea automată a emailurilor la nivelul staţiei 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 şi a euristicii de detecţie a acestui tip de programe, produsul va trebui să ofere protecţie anti-spyware;

• Setarea priorităţilor scanărilor programate;

• Soluţia trebuie să permită configurarea mecanismelor de scanare utilizând tehnologii locale, bazate pe cloud sau alte mecanisme echivalente oferite de producător, pentru optimizarea performanţei şi consumului de resurse;

• Administratorul trebuie să poată configura politicile şi mecanismele de scanare disponibile, inclusiv utilizarea tehnologiilor locale, bazate pe cloud sau a altor mecanisme echivalente, în funcţie de infrastructura protejată şi recomandările producătorului;

• Setarea a tipurilor de detecţie: bazate pe semnături, bazate de comportamentul fişierelor şi bazate pe monitorizarea proceselor;

• Scanarea paginilor web;

• Setarea a unei parole pentru protecţia la dezinstalare;

• Modul de antiphishing;

• Protecţie în timp real pe maşinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată;

• Soluţia trebuie să suporte implementarea în medii VDI persistente şi non-persistente, inclusiv utilizarea imaginilor de referinţă *(Golden Image/Template)* sau a unor mecanisme echivalente oferite de producător;

• Utilizarea uni modul adiţional de securitate bazat pe algoritmi tunabili de machine learning respectiv algoritmi euristici agresivi capabili să detecteze şi blocheze atacuri de tip persistent sau targetat precum şi alte categorii de malware sofisticat înainte de faza de execuţie. Acest modul oferă următoarele funcţionalităţi:

***a)*** *clasificarea tipului de atac;*

***b)*** *abilitatea de a configura acţiunile aplicate ameninţărilor detectate, inclusiv raportarea, monitorizarea sau blocarea acestora;*

***c)*** *abilitatea de a configura nivelul de sensibilitate al mecanismelor de detecţie şi politicilor de securitate, conform recomandărilor producătorului;*

***d)*** *abilitatea de a acţiona în mod diferit în funcţie de tipul ameninţării (fişier sau atac prin reţea);*

• Posibilitatea de restaurare a fişierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, cînd determină că procesul este maliţios;

• Oprirea atacurile avansate de tip „zero-day” efectuate prin intermediul unor exploit-uri evazive;

• Depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare;

• Protejarea aplicaţiilor utilizate frecvent şi a celor de tip „sistem" cum ar fi browserele, aplicaţiile de tip office sau reader, procesele critice aferente sistemelor de operare.

## ***Firewall:***

• Sa ofere posibilitatea de a configura reguli de firewall pentru aplicaţii sau conectivitate;

• Modulul să poată fi instalat/ activat/ dezactivat/ dezinstalat la cerere;

• Să permită definirea de reţele de încredere pentru maşina destinaţie.

## ***Protecţia datelor:***

• Produsul trebuie să permite blocarea datelor confidenţiale *(pin-ul cardului, cont bancar etc)* transmise prin HTTP sau SMTP prin crearea unor reguli specifice.

## ***Controlul conţinutului:***

Produsul trebuie să ofere un modul integrat dedicat controlului accesului la Internet cu următoarele particularităţi: blocarea accesului la Internet pentru anumite maşini client sau grupuri de maşini, blocarea accesului la Internet pe intervale orare, blocarea paginilor de internet care conţin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, blocarea accesului la anumite aplicaţii definite de administrator, restricţionarea accesului pe anumite pagini de internet după anumite categorii prestabilite *(ex: online dating, violenta, pornografie etc).*

## ***Controlul dispozitivelor:***

Produsul trebuie să conţină 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 maşina client;

• Permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

## ***Power User:***

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

• Poată fi instalat/dezinstalat în funcţie de preferinţa administratorului;

• Permită posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa şi modifica setările clientului antivirus dintr-o consola disponibilă local pe maşina client;

• Permită administratorului soluţiei să suprascrie din consola setările aplicate de utilizatorii Power User**.**

## ***Actualizare:***

Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor:

• La nivel de staţie în mod silenţios *(fără avertizări);*

• Folosind unul sau mai multe servere de actualizare;

• Pentru locaţiile la distanţă prin intermediul unui client antivirus care are şi rol de server de actualizare.

• Gestionabil – doar local sau şi servere online.

## ***Protecţie Anti-Tampering:***

• Va permite detecţia driverelor vulnerabile pe dispozitivele conectate *(endpointuri)* şi când sunt efectuate încercări avansate de atac pentru a dezactiva agentul de securitate, ceea ce poate duce la compromiterea integrităţii produsului;

• Va permite detectarea de drivere vulnerabile pe dispozitivele conectate care pot fi exploatate de atacatori, reprezentând ameninţări la adresa integrităţii produsului. Tehnologia este compatibilă cu sistemele de operare Windows şi Linux;

• Va fi capabilă să protejeze împotriva ameninţărilor noi sau erorilor umane neintenţionate ce ar putea fi proiectate pentru a permite acces neautorizat la kernel, ducând la compromiterea integrităţii poate detecta când funcţiile de tip callback ale agentului de securitate au fost eliminate sau dezactivate în mod maliţios.

## ***Disk Encryption:***

Soluţie pentru managementul criptării discurilor pentru 1000 entităţi.

Soluţia va oferi următoarele funcţionalităţi minime:

• Administrarea produsului trebuie să fie realizată din aceeaşi consolă de management ca şi soluţia de protecţie antivirus;

• Produsul va utiliza mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows şi FileVault pentru Mac OSX;

• Va asigura vizibilitatea completă asupra stării de criptare a dispozitivelor inclusiv: numele staţiei, IP-ul staţiei, sistemul de operare, ID-ul volumului/partiţiei, numele partiţiei, starea criptării partiţiei, tipul partiţiei: boot, non-boot, mărimea partiţiei în GB, ID-ul cheii de recuperare;

• Produsul trebuie să asigure criptarea pentru Următoarele OS: Windows 7/10/11 Pro/Enterprise *(with TPM)*; WindowsServer 2012/2012 R2, 2016, 2019, 2022 *(with TPM)*, OSX de la 10.12.

## **Alte cerinţe:**

Perioada de suport şi menţinere de la producător:

**1.** Pentru soluţia ofertată se solicită a fi 36 luni;

**2.** Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanţă.

***Notă:*** *Lucrările de instalare, configurare, punerea în funcţiune a soluţiei trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă.*