Anexa nr. 21
la Documentația standard nr. 115
din "15" septembrie 2021

CAIET DE SARCINI

Obiectul: Software antivirus, cu perioada de valabilitate a licențelor 36 luni

Autoritatea contractantă: S.A. „Furnizarea Energiei Electrice Nord", mun. Bălți, str. Strîi, 17A

Tipul principal de activitate: furnizarea energiei electrice

Numărul de telefon/fax: 023164307, 062163403, 068768833

Adresa de e-mail și pagina web oficială ale autorității contractante la care se va putea obține accesul la documentația de atribuire: anticamera@fee-nord.md , https://fee-nord.md/achizitii/

Caietul de sarcini face parte integrantă din documentele procedurii de achiziții, organizate de S.A. „FEE-Nord" (în continuare "Beneficiar" sau "Autoritate Contractantă") și cuprinde: descrierea obiectului achiziției, criteriile de calificare și selecție, documentele de calificare, etc.

1. Descriere generală. Informații

Achiziția software antivirus, cu perioada de valabilitate a licențelor 36 luni, pentru:
- 90 stații de lucru fizice si virtualizate;
- 3 servere fizice si virtualizate.

Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaţionale independente cu renume mondial în domeniu (certificări AV-TEST, AV-Comparatives, etc.)

*** Notă:** Nu se admit la concurs ofertele care propun soluți software produse în Federația Rusă, sau de proveniență rusă, sau de către companii cu capital provenit din Federația Rusă.

Restricția se impune în conformitate cu scrisoarea Ministerului Energiei al Republicii Moldova nr. 07-1973 din data de 23.11.2023 (anexată la prezentul caiet de sarcini), și recomandarea Serviciului de Informații și Securitate nr. E/5729 din 05.07.2023 (anexată la prezentul caiet de sarcini), de a evita utilizarea produselor și soluțiilor de securitate dezvoltate în Federația Rusă, sau de proveniență rusă, sau de către companii cu capital provenit din Federația Rusă, și admiterea în concurs doar a produselor și soluțiilor de securitate cibernetică dezvoltate de companii cu o reputație ireproșabilă din țările cu o democrație dezvoltată precum Uniunea Europeană, SUA, Canada, Japonia, etc.

Caracteristici generale ale produsului:

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:

- Windows 10, 8.1, 7 sau mai recent.
- Windows Server 2012 R2/2016/2019.
- 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.
- Sa poata face actualizări automate a consolei de management de către producătorul soluţiei, fara a fi necesara intervenţia utilizatorului.

- Consola de management sa fie accesibila de oriunde in lume (sa fie bazata pe un serviciu cloud de tip Software-as-a-Service), fara a fi nevoie de setări suplimentare din partea utilizatorului.

Consola de management:

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

Consola de management va fi oferita cu o baza de date inclusă, non-relaţională.
Soluţia trebuie să:

- fie scalabilă, astfel ca oricare dintre roluri sau servicii să poată fi instalate separat sau împreună pe aceeaşi sau mai multe VDI-uri.
- asigure următoarele roluri: server cu baza de date, server de comunicaţie, server de actualizare, server de web.
- asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale VMware şi Citrix prin task din consola de management.
- includă un modul load balancer pentru performanţă şi redundanţă.
- includă mecanisme de configurare a disponibilităţii pentru serverul cu baze de date (clustering).
- includă posibilitatea de a fi accesată atât de pe staţiile de lucru cât şi de pe dispozitivele mobile (tabletă, smartphone).

Limba interfeţei consolei de management va putea fi selectată dintre limbile româna sau engleză. Limba interfeţei agentului care se instalează pe statii de lucru și servere, va putea fi selectată dintre limbile româna sau engleză.

Cerinţe generale produs:

Soluţia trebuie să:

- includă unul sau mai multe module de update server prin care să asigure actualizarea componentelor şi a semnăturilor.
- permită activarea/dezactivarea actualizărilor automate de produs/semnături şi a consolei de management.
- transmită alerte de ne funcţionalitate, cu 30 de minute înainte de actualizare.
- permită 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).
- permită integrarea cu un server Syslog pentru raportarea evenimentelor antivirus.
- permită instalarea serviciului de SMNP pentru raportarea statusului maşinilor din cadrul componentei de management.

Inventarierea rețelei - managementul securității:

Produsul trebuie să:

- se integreze cu domenii Active Directory multiple, VMwaie vCenter, Citrix Xen şi să importe inventarul acestor platforme.
- permită descoperirea maşinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.
- permită descoperirea staţiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery.
- ofere opţiuni de căutare, sortare şi filtrare după numele sistemului, sistem de operare și adresă IP.
- 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 actualizări, Versiunea produsului, Versiunea de semnături.
- permită descoperirea tuturor aplicaţiilor instalate pe toate staţiile şi serverele din reţea.
- permită crearea unui pachet unic pentru toate sistemele de operare, de staţii sau servere. Astfel, administratorul va putea descarcă pachetele pentru protecţia staţiilor si serverelor pe care rulează sistemul de operare Windows și Linux.

Politici:

Produsul trebuie să:

- permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conţine setări pentru toate modulele.
- 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 același reţea cu infrastructura de management, Tipul reţelei (lan, wireless).

Rapoarte:

Produsul trebuie să:

- conţină rapoarte care prezintă statusul maşinilor clienţii din punct de vedere al actualizărilor, fişierelor malware detectate, aplicaţiile blocate, site-urilor web blocate.
- transmită rapoartele programate către un număr nelimitat de adrese de email (ne fiind nevoie să posede un cont în consolă de management).
- permită vizualizarea rapoartelor curente programate de administrator.
- permită exportarea rapoartelor în format .pdf si detaliile ca format .csv.

Carantină:

- produsul trebuie să permită restaurarea fişierelor din carantină în locaţia originală sau într-o cale configurabilă.
- locaţia, fişierele şi administrarea Carantinei trebuie să fie efectuată central 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.

Log-uri:

- soluţia trebuie să permită înregistrarea acţiunilor utilizatorilor şi să ofere informaţii detaliate

pentru fiecare acţiune a unui utilizator cu posibilitatea de filtrare.

Actualizări:

Soluţia trebuie să:

- permită definirea locaţiilor de actualizare multiple.
- permită activarea/dezactivarea actualizărilor de produs și semnături.
- ofere posibilitatea ca orice client antivirus să poată fi configurat, să ofere update-urile către alt client antivirus.
- permită testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din reţea, evitând posibilele probleme ce pot afecta serverele sau staţiile critice. Astfel, serverul de actualizare va include 2 tipuri de actualizări de produs:
  a. ciclu rapid, gândit pentru un mediu de test în cadrul reţelei;
  b. ciclu lent, gândit pentru restul reţelei (producţie, servere critice, etc.);
- permită stabilirea zonelor de test și critice din cadrul reţelei prin intermediul politicilor din consola de management.

Protecţie stafii si servere fizice si virtualizate - caracteristici minime:

Soluţia antivirus trebuie să:

- permită instalarea personalizată a modulelor deţinute (de exemplu, sa permită instalarea soluţiei antimalware fără modulul de control al accesului web, modulul de control al dispozitivilelor sau modulul firewall).
- să includă un vaccin anti-ransomware, pentru o mai buna protecţie a stațiilor și serverelor. Acest vaccin va asigura protecţia impotriva tuturor ameninţărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare.
- vaccinul anti-ransomware trebuie să primească actualizări de la producător, odata cu actualizarea semnaturilor produsului Antimalware.
- pentru o mai buna protecţie a stațiilor și serverelor, soluţia trebuie să includă protecţie împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazată pe tehnologii de invățare automată (machine learning).
- pentru o mai bună protecţie a staţiilor și serverelor, soluţia trebuie să includă un modul integrat de tip ERA (Endpoint Risk Analytics - Analiza de risc a endpoint-ului) capabil să identifice și remedieze în mod automatizat sau manual un număr mare de riscuri existente la nivel de reţea sau sistem de operare ce pot afecta funcţionalitatea și nivelul de securizare al endpoint-ului.

Administrare și instalare remote:

- înainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
- instalarea se va putea face în mai multe moduri:
  a. prin descărcarea directă a pachetului pe stația pe care se va face instalarea;
  b. prin instalarea la distanță, direct din consola de management;
  c. trimiterea pe email (oricâte adrese) a pachetului de instalare pentru Windows și Linux.
- instalarea clienţilor la distanță în alte locaţii decât cele în care este instalată consola de management se va face prin intermediul unui client existent în locaţiile respective de tip relay pentru a minimiza traficul în WAN.
- în consolă vor fi disponibile informaţii despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicată, informaţii despre actualizări, etc.
- din consolă se va putea trimite o singura politică pentru configurarea integrală a clientului de pe stații/servere.
- consola va include o secţiune, „Audit”, unde se vor menţiona toate acţiunile întreprinse fie de

administratori fie de reporteri, cu informaţii detaliate: logare, editare, creare, delogare, mutare etc.

- posibilitatea creări unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biţi cât și pentru cele pe 64 de biţi.
- posibilitatea creări unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), servere (fizice și/sau virtuale).
- posibilitatea de a crea pachete de instalare de tip web installer sau kit full.
- administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta stațiile/serverele din reţea pentru cele care nu sunt integrate domeniu.
- să permită selectarea clientului care va realiza descoperirea stațiilor din reţea, altele decât cele integrate în domeniu.

<u>Caracteristici si funcţionalităţi principale ale modulului antivirus:</u>

Produsul trebuie sa permită:

1. Administratorului sa stabilească acţiunea luată de produsul Antimalware la detectarea unei ameninţări noi. Astfel administratorul va putea alege între următoarele acţiuni:
   a. Acţiune imiplicita pentru fişiere infectate:
      - interzice accesul
      - dezinfectează
      - ştergere
      - mută fişierele în carantină
      - nicio acţiune
   b. Acţiune alternativă pentm fişierele infectate:
      - interzice accesul
      - dezinfectează
      - ştergere
      - mută fişierele în carantină
   c. Acţiune imiplicită pentru fişierele suspecte:
      - interzice accesul
      - ştergere
      - mută fişierele în carantină
      - nicio acţiune
   d. Acţiune alternativă pentru fişierele suspecte:
      - interzice accesul
      - ştergere
      - mută fişierele în carantină
2. Scanarea automată în timp real va putea fi setată să nu scaneze arhive sau fişiere mai mari de «X» MB, mărimea fişierelor putând fi definită de administratorul soluţiei.
3. Definirea până la 16 nivele de profunzime pentru scanarea în arhive.
4. 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 semnătură nu a fost lansată încă.
5. Scanarea oricărui suport de stocare a informaţiei (CD-uri, harduri externe, unitari partajate etc). De asemenea, se va putea anula scanarea în cazul în care sunt detectate unități care au informaţii stocate mai mult de «X» MB.
6. Scanarea automată a emailurilor la nivelul statiei de lucru pentru POP3/SMTP.
7. Configurarea căilor ce urmează a fi scanate la cerere.
8. Clienţii antimalware pentru workstation să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fişiere, extensii sau procese.
9. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecţie a acestui tip de programe, produsul va trebui să ofere protecţie anti-spy ware.

10. Posibilitatea de a configura scanările programate să se execute cu prioritate redusă.
11. Produsul antimalware să poată fi configurat să folosească scanarea în cloud, și parţial scanarea locală.
12. Administratorul poate personaliza şi motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:
    - scanare locală, când scanarea se efectuează pe staţia de lucru locală.
    - scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud şi, parţial, semnături locale.
13. Pentru o protecţie sporită, soluţia antimalware trebuie să dispună de 3 tipuri de detecţii: 1. bazată pe semnături, 2. bazată pe comportamentul fişierelor, si 3. bazată pe monitorizarea proceselor.
14. Pentru o protecţie sporită, soluţia antimalware trebuie sa poată scana paginile HTTP.
15. Pentru o mai bună gestionare a antimalware instalat pe statii, produsul va include opţiunea de setare a unei parole pentru protecţia la dezinstalare.
16. Pentru siguranţa utilizatorului, clientul va include un modul de antiphishing.
17. Soluţia oferă protecţie in timp real pe maşinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata.

Firewall:

- să ofere posibilitatea de a configura reguli de firewall pentru aplicaţii sau conectivitate.
- modulul să poată fi instalat/dezinstalat la cerere.
- să permită definirea de reţele de încredere pentru maşina destinaţie.

Carantina:

Produsul trebuie sa permită:

- trimiterea automata a fişierelor din carantina către laboratoarele antimalware ale producătorului.
- trimiterea conţinutului carantinei și care va putea fi expediat în mod automat, la un interval definit de administrator.
- ștergerea automată a fişierelor carantinate mai vechi de o anumită perioadă, pentru a nu încarca inutil spaţiul de stocare.
- posibilitatea de a restaura un fişier din carantină în locaţia lui originală.
- rescanarea obiectelor după fiecare actualizare de semnaturi a modulululului de carantină.

Protecţia datelor:

- Produsul trebuie să permite blocarea datelor confidenţiale (pin-ul cârdului, 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 (de exemplu, online dating, violență, pornografie, etc.).

Controlul aplicaţiilor:

Pentru administrare şi inventariere eficientă produsul trebuie să deţină un modul care va oferi posibilitatea de a:

- efectua descoperirea aplicaţiilor utilizate pe staţiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe.
- regăsi toate procesele descoperite în reţea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe.
- bloca rularea anumitor aplicaţii sau procese definite de administrator (inclusiv subprocese) după: cale fişier: local, CD-ROM, portabil sau reţea, hash, certificat.

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, TapeDrives, Windows Portable, COM/LPT Ports, SCSI Raid, Printers, Network Adapters, Wireless Network Adapters, Internai and Externai 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 consolă disponibilă local pe maşina client.
- permită administratorului soluţiei să suprascrie din consolă 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.

Alte cerințe:

Perioada de suport local si menţinere de la producător:

- pentru soluţia ofertată se solicită ca produsul sa fie aliniat la perioada de valabilitate a licențelor existente.
- producătorul trebuie să ofere suport 24/24, prine-e-mail sau conectare de la distanţă, inclusiv suport local în limba română din partea partenerului.
- partenerul va prezenta autorizarea de la producător pentru produsul ofertat;
- partenerul va prezenta minim 2 certificate tehnice a persoanelor certificate pe produsul ofertat.

Se va oferi manual de instalare si administrare în limba româna și/sau rusă și engleză pentru produsul ofertat.

2. Cerințe față de operatorii economici:

a) experienţa în domeniu, nu mai puțin de 3 ani;
b) să dispună de toate documentele permisive necesare (licențe, acreditări, atestări, ș.a.) pentru practicarea genului de activitate și comercializarea produsului solicitat;
c) să dispună de o bună reputație și o experiență de subscriere.

3. Documente obligatorii la depunerea ofertei

1. Cerere de participare (Anexa nr. 7 la Documentația standard);
2. Declarația privind valabilitatea ofertei (Anexa nr. 8 la Documentația standard);
3. Specificații tehnice (Anexa nr. 22 la Documentația standard);
4. Specificații de preț (Anexa nr. 23 la Documentația standard);
5. Declarație de eligibilitate (Anexei nr. 2 la Regulamentul cu privire la achizițiile publice de valoare mica);
6. Declarație privind confirmarea identității beneficiarilor efectivi și neîncadrarea acestora în situația condamnării pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă şi/sau spălare de bani (formular aprobat prin Ordinul Ministrului Finanțelor nr. 145 din 24 noiembrie 2020);
7. Copia extrasului din Registrul de Stat al persoanelor juridice, conținând ultimele modificări la data depunerii ofertei;
8. Copia actului confirmativ al parteneriatului autorizat, eliberat de Producătorul produsului ofertat, ce atestă dreptul de a livra produsul ofertat, semnată cu aplicarea semnăturii electronice avansate calificate;
9. Certificat tehnic pentru produsul ofertat;
10. Actele de certificare tehnică a cel puțin 2 specialiști pentru produsul ofertat;
11. Copia raportului financiar pentru anul 2022, înregistrat la Biroul Național de Statistică;
12. Declarație privind lista principalelor livrări/prestări efectuate în ultimii 2 ani de activitate (Anexa nr. 12 din Documentația standard);
13. Formularul standard al DUAE, care va cuprinde:
    - Informații referitoare la operatorul economic (Capitolului II. din Formularul DUAE);
    - Motive de excludere din cadrul procedurii de achiziție publică (Capitolului III. din Formularul DUAE);
    - Criteriile de calificare și selecție a operatorilor economici (Capitolului IV. din Formularul DUAE);
    - Indicații generale pentru criteriile de calificare și selecție (Capitolului V. din Formularul DUAE).

Notă: Toate documentele urmează a fi semnate electronic de către conducătorul operatorului economic sau de către persoana împuternicită de acesta, anexând, totodată și documentul confirmativ (procura) ce ar atesta delegarea persoanei în cauză.

4. Criteriul de evaluare aplicat pentru atribuirea contractului

Oferta determinată ca fiind în mod substanţial neconcordantă poate fi respinsă de către Beneficiar şi discordanţa nu poate fi ulterior corectată de către Ofertant.

Va fi selectată oferta cu cel mai scăzut preț ofertat, fără TVA.

Factorii de evaluare a ofertelor și ponderile lor

Nr. d/o	Denumirea factorului de evaluare	Ponderea, %
1.	Prețul ofertei	100%

1.

5. Limba sau limbile în care trebuie redactate ofertele sau cererile de participare

Limba romană.

Digitally signed by Schița Sergiu
Date: 2023.12.11 14:55:00 EET
Reason: MoldSign Signature
Location: Moldova

Șef Secție Tehnologii Informaționale I. Crutoi

Autoritatea contractantă _____

Ministerul Energiei
al Republicii Moldova

Nr. 07-1973 din 23 noiembrie 2023

Conform listei

Prin prezenta, având în vedere importanța vitală de asigurare a securității cibernetice în sectorul energetic și obiectivul de a menține funcționarea fiabilă și continuă a infrastructurilor critice TIC și SCADA deținute de entitățile din sectorul energiei care au în gestiune obiective de infrastructură critică de importanță națională, Ministerul Energiei Vă aduce la cunoștință despre recomandările expuse prin demersul nr. E/5729 din 5 iunie 2023 al Serviciului de Informații și Securitate *(se anexează),* privind necesitatea de a evita utilizarea produselor și soluțiilor de securitate dezvoltate în Federația Rusă *(se anexează)*.

Entitățile deținătoare de obiective de infrastructură critică de importanță națională, la etapele de planificare, inițiere și desfășurare a procedurilor de achiziții, se recomandă să se ia în considerare nu doar criteriul prețului cel mai scăzut, ci și alte criterii, cum ar fi obținerea celui mai bun raport calitate-preț cu suficiente criterii de eligibilitate și factori de evaluare după cum urmează:

a) calitatea, inclusiv avantajele tehnice, caracteristicile funcționale, accesibilitatea, precum și originea de comercializare și condițiile acesteia;

b) organizarea, calificarea și experiența personalului desemnat pentru executarea contractului, în cazul în care calitatea personalului desemnat are un impact semnificativ asupra nivelului calitativ de executare a contractului;

c) serviciile post-vânzare, asistența tehnică și condițiile de livrare, cum ar fi data livrării, procesul de livrare și termenul de livrare sau de finalizare;

Totodată, luând în considerare măsurile restrictive menționate supra, se vor admite doar soluțiile și produsele de securitate cibernetică, dezvoltate de companii cu o reputație ireproșabilă din țări cu o democrație dezvoltată, precum: state din Uniunea Europeană, Statele Unite ale Americii, Canada, Japonia, etc.

Piața Marii Adunări Naționale 1, mun. Chișinău, MD-2012, tel. +373-22-25-01-31, fax +373-22-23-40-64
E-mail: secretariat@energie.gov.md Pagina web: www.energie.gov.md

Urmare celor menționate și în contextul geopolitic actual, solicităm respectuos entităților din sectorul energetic să se conducă cu strictețe de aceste măsuri restrictive în ceea ce ține de utilizarea produselor software și soluțiilor TIC de securitate cu proveniența din Federația Rusă sau a companiilor cu capital provenit din Federația Rusă.

În conchidere, Vă informăm, că Ministerul Energiei este în proces de coordonare cu alte autorități și instituții publice responsabile de domeniul de securitate cibernetică și națională, pentru aprobarea cadrului de reglementare care să stabilească expres astfel de restricții de a nu admite produse și soluții de origine din Federația Rusă în sectorul energetic pentru atingerea scopului imperativ de protecție a infrastructurilor critice la nivel național.

Anexe: 1) *Demersul nr. E/5729 din 5 iunie 2023 al Serviciului de Informații și Securitate – 1 (una) filă;*

2) *Lista privind produsele, aplicațiile și sistemele de securitate cibernetică interzise în sectorul energiei – 3 (trei) file.*

Secretar de Stat **Cristina PERETEATCU**

Ex. Gheorghe VÎRLAN, Tel. (022)-250-664

Piața Marii Adunări Naționale 1, mun. Chișinău, MD-2012, tel. +373-22-25-01-31, fax +373-22-23-40-64
E-mail: secretariat@energie.gov.md Pagina web: www.energie.gov.md

Lista de distribuire a demersului nr. 07-1973 din 23 noiembrie 2023

1. *Copie:* **Agenția Naționale pentru Reglementare în Energetică**
   e-mail: anre@anre.md
2. *Copie:* **Serviciul de Informații și Securitate**
   e-mail: sis@sis.md
3. **Agenția pentru Eficiență Energetică**
   e-mail: office@aee.md
4. **ÎCS „Premier Energy" SRL**
   e-mail: servicii_client@premierenergy.md
5. **ÎCS „Premier Energy Distribution" SA**
   e-mail: OT24@premierenergy.md
6. **SA „FEE-Nord**"
   e-mail: anticamera@fee-nord.md
7. **SA „RED-Nord"**
   e-mail: anticamera@rednord.md
8. **ÎS „Moldelectrica"**
   e-mail: cancelar@moldelectrica.md
9. **SA „Energocom"**
   e-mail: office@energocom.md
10. **SA „Termoelectrica"**
    e-mail: cancelaria@termoelectrica.md
11. **SA „CET-Nord"**
    e-mail: office@cet-nord.md
12. **SRL „Vestmoldtransgaz"**
    e-mail: office@vmtg.md
13. **Nodul Hidroenergetic Costești**
    e-mail: i.s.nodulhidroenergetic@gmail.com
    info@nhec.md

Anexa nr. 2
la demersul nr. 07-1973 din 23 noiembrie 2023

LISTA
privind produsele, aplicațiile și sistemele de securitate cibernetică interzise în sectorul energiei

Nr.	Denumirea a produselor, aplicațiilor și sistemelor de Securitate cibernetică	Elemente de identificare	URL/site
1.	XSIGNAL • Serviciu	19801, US, Delaware, 919, Wilmington, North Market Street, 950	https://xsignal.io/ https://bit-signal.ru/
2.	Metascan • Serviciu	Krasnohorsk Street, Egorova 5 Moscow, Russia TIN 5024179758 KPP 502401001 PSRN 1175024028772	https://metascan.ru/
3.	Dr. Web • Dr.Web Control Center • Dr.Web Desktop Security Suite • Dr.Web Server Security Suite • Dr.Web Mail Security Suite • Dr.Web Gateway Security Suite • Dr.Web Mobile Security Suite • Dr.Web KATANA • Dr.Web Security Space (for Windows) • Dr.Web Security Space (for Linux) • Dr.Web Security Space (for macOS) • Dr.Web Security Space (for MS-DOS, OS/2) • Dr.Web Security Space (for Android)	Global HQ, 125124, 3rd street Yamskogo polya 2-12A, Moscow Russia	https://www.drweb.com/
4.	Kaspersky Security • Kaspersky Anti-Virus • Kaspersky Internet Security • Kaspersky Total Security • Kaspersky Security Cloud Personal • Kaspersky VPN Secure Connection • Kaspersky Password Manager • Kaspersky Safe Kids • Kaspersky Internet Security for Mac • Kaspersky Internet Security for	Leningradskoye Hwy, 39A строение 2, Moskva, Rusia, 125212	https://www.kaspersky.com/

	Android • Kaspersky Virus Removal Tool • Kaspersky Rescue Disk		
5.	RPA RusBITech JSC RusBITech Astra • ПТК Каркас-С - PTK Karkas-S • КП СГП Комплекс программ «Специальный генератор паролей» - KP SGP Complex de programe „Generator de parole speciale”	117105, Moscow, Varshavskoye shosse, 26, building 11	https://rusbitech.ru/
6.	Infotecs • ViPNet Coordinator HW • ViPNet xFirewall • ViPNet EndPoint Protection • ViPNet Coordinator IG • ViPNet SIES • ViPNet OSSL • ViPNet TIAS • ViPNet Client for mobile platforms • ViPNet Client for workstations • ViPNet Coordinator IG • ViPNet Coordinator HW • ViPNet Coordinator KB • ViPNet Coordinator VA • ViPNet CSP 4 • ViPNet EndPoint Protection • ViPNet IDS HS • ViPNet IDS MC (Management Center) • ViPNet IDS NS • ViPNet Password Generator • ViPNet Personal Firewall 4 • ViPNet PKI Client • ViPNet PKI Service • ViPNet Policy Manager • ViPNet Quantum Trusted System (ViPNet QTS) • ViPNet QTS Lite • ViPNet Quandor 2 • ViPNet SafeBoot • ViPNet SafePoint • ViPNet SIES • ViPNet Statewatcher • ViPNet Terminal • ViPNet TIAS ViPNet TLS Gateway	127273, Moscow, st . Otradnaya, 2B str. 1	https://infotecs.ru/
7.	Era Technopolis	Adresa sediului principal: Federaɯia Rusĉ, Krasnodar,	https://mil.ru/era.htm

		Bulevardul Pionerskiy, 41	
8.	Pasit Ao	Adresa sediului principal: Federaɯia Rusĉ, Moscova, Bulevardul Lenin, 30	https://pasit.ru/
9.	Neobit, 000	Adresa sediului principal: Federaɯia Rusĉ, Saint Petersburg, strada Gzhatskaya, 21	https://neobit.ru/
10.	Advanced System Technology, Ao	Adresa sediului principal: Federaɯia Rusĉ, Moscova, Autostrada Kashirskoye, 3k2	https://acti.ru/
11.	Positive Technologies, Ao	Adresa sediului principal: Federaɯia Rusĉ, Moscova, Autostrada Shchelkovskoe, 30	https://www.ptsecurity.com/ww-en/

SERVICIUL DE INFORMAȚII ȘI SECURITATE
AL REPUBLICII MOLDOVA

MD-2004, mun.Chișinău, bd. Ștefan cel Mare și Sfînt, 166, tel. 022-239-625, fax. 022-234-068 e-mail: sis@sis.md

„05” iunie 2023 Nr. E/5729

La nr. 07-562 din 30.05.2023.

Domnului Victor PARLICOV
Ministrul Energiei

Stimate domnule Parlicov,

În conformitate cu solicitarea parvenită Serviciul de Informații și Securitate vă comunică că, în contextul geopolitic actual, utilizarea unor servicii IT și produse software care sunt produse în F. Rusă sau de companii cu capital provenit din F. Rusă implică riscuri majore de securitate pentru sistemele TIC și SCADA din cadrul infrastructurilor critice, inclusiv în sectorul energetic. În acest sens, **se va evita utilizarea** soluțiilor de securitate produse de companiile **Kaspersky**, **Dr. Web**, **Infotecs** *(soluțiile ViPNet)*, **Neobit**, **Positive Technologies** *(suita de soluții PT și MaxPatrol)* și se vor utiliza soluții alternative dezvoltate de companii cu o reputație ireproșabilă din țări cu o democrație dezvoltată (UE, SUA, Canada, Japonia etc.).

Atragem atenția că, lista companiilor menționate supra nu este una exhaustivă, fiind prezentate doar unele din cele mai cunoscute.

Cu respect,

Alexandru MUSTEAȚA
Director