ANUNȚ DE PARTICIPARE

privind achiziționarea: Servicii de prevenire a pierderilor de date (DLP)

prin procedura de achiziție: Valoare mică

***Procedura a fost inclusă în planul de achiziții publice a autorității contractante (Da/Nu):** Da
Link-ul către planul de achiziții publice publicat: *https://sfs.md/ro/rapoarte-pe-achizitii*

1. **Denumirea autorității contractante:** SERVICIUL FISCAL DE STAT
2. **IDNO:** 1006601001182
3. **Adresa:** mun. Chișinău, str. Constantin Tănase, nr. 9
4. **Numărul de telefon/fax:** 022-82-32-92, 82-32-63
5. **Adresa de e-mail şi pagina web oficială autorității contractante***: mail@sfs.md*, *www.sfs.md*
6. **Adresa de e-mail sau pagina web oficială de la care se va putea obține accesul la documentația de atribuire:** *documentația de atribuire este anexată în cadrul procedurii în SIA RSAP*
7. **Tipul autorității contractante și obiectul principal de activitate (dacă este cazul, mențiunea că autoritatea contractantă este o autoritate centrală de achiziție sau că achiziția implică o altă formă de achiziție comună):** Instituție publică, obiectul principal de activitate: Administrarea operațiunilor fiscale
8. **Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind livrarea/prestarea următoarelor bunuri/servicii:**

Nr. d/o	Cod CPV	Denumirea bunurilor	Unitatea de măsură	Cantitatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată fără TVA, lei
1.		**Lotul 1**				
1.1.	48200000-0	**Servicii de prevenire a pierderilor de date (DLP)**	Buc.	100 stații	Conform cerințelor solicitate în caietul de sarcini (Anexa nr. 1) pentru soluția de software DLP (Soluția de prevenire a pierderilor de date Data Loss Prevention DLP)	160 000,00
Valoarea estimativă totală						**160 000,00**

9. **În cazul în care contractul este împărțit pe loturi un operator economic poate depune oferta:**
   1) Pentru un singur lot;
10. **Termenii și condițiile de livrare/prestare solicitați:** Prestatorul v-a asigura livrarea, instalarea, și configurarea soluției DLP (Data Loss Prevention), în termen de 15 zile de la data înregistrării Contractului la Trezoreria Regională Chișinău.
11. **Termenul de valabilitate a contractului:** 31.12.2024;
12. **Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora și a criteriilor de selecție/de preselecție; 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.	**(DUAE) - Documentul unic de achiziții european**	Formular completat - confirmat prin aplicarea semnăturii electronice de către administratorul companiei indicat în Extrasul Registrului de Stat al persoanelor juridice sau de către persoana împuternicită.	Obligatoriu
2.	**Specificația tehnică**	Confirmat prin aplicarea semnăturii electronice de către administratorul companiei indicat în Extrasul Registrului de Stat al persoanelor juridice sau de către persoana împuternicită; *Conform anexei nr. 22 din Documentația Standard aprobată prin Ordinul Ministerului Finanțelor nr. 115 din 15.09.2021.*	Obligatoriu
3.	**Specificația de preț**	Confirmat prin aplicarea semnăturii electronice de către administratorul companiei indicat în Extrasul Registrului de Stat al persoanelor juridice sau de către persoana împuternicită; *Conform anexei nr. 23 din Documentația Standard aprobată prin Ordinul Ministerului Finanțelor nr. 115 din 15.09.2021.*	Obligatoriu
4.	**Garanția pentru ofertă 2%**	2.0% din valoarea ofertei fără TVA. -În cazul în care garanția bancară urmează a fi prezentată conform anexei nr. 9 din Documentația Standard aprobată prin Ordinul Ministerului Finanțelor nr. 115 din 15.09.2021, valabilă 45 zile, - În cazul garanției pentru ofertă sub formă de transfer bancar, conform următoarelor date bancare: Beneficiarul plății: Serviciul Fiscal de Stat Denumirea Băncii: Ministerul Finanţelor - TR Chișinău buget de stat Codul fiscal:1006601001182 Contul de decontare; MD58TRPCAA518410A01191AA operatorul economic v-a prezenta ordinul de plată cu confirmarea de către bancă a executării plății până la termenul limită de depunere a ofertei. copie confirmat prin aplicarea semnăturii electronice de către administratorul companiei indicat în Extrasul Registrului de Stat al persoanelor juridice sau de către persoana împuternicită atât și în cazul delegării sau împuternicirii persoanei.	Obligatoriu
5.	**Extras din Registrul de stat al persoanelor juridice**	Copia documentului confirmativ confirmat prin semnătura electronică a operatorului economic	Obligatoriu
6.	**Certificat de conformitate sau echivalent ce confirmă calitatea bunului (ISO sau certificate similare)**	Copie certificat valabil sau document valabil echivalent ce confirmă calitatea bunului (ISO sau certificate de calitate similare).	Obligatoriu
7.	**Autorizare de la producător**	Copia acordului de parteneriat cu compania producătoare sau a altui document ce confirmă dreptul ofertantului de livrare autorizat de producător.	Obligatoriu
8.	**Declarația de eligibilitate**	Se va prezenta de către ofertantul desemnat câștigător în termen de 3 zile de la data comunicării rezultatelor procedurii de achiziție publică, în adresa autorității contractante (SFS), conform modelului aprobat prin HG 870 din 14.12.2022, Anexa nr. 2, semnat în format electronic.	Obligatoriu

13. **Garanția pentru ofertă, cuantumul:** în cuantum de 2 % din valoarea ofertei fără TVA;

14. **Tehnici și instrumente specifice de atribuire (după caz, specificați dacă se va utiliza licitația electronică):** licitaţie electronică – 3 runde. Pasul minim de micşorare a ratei de licitaţie este 1 % per lot;

15. **Ofertele se prezintă în valuta:** Lei MD;

16. **Criteriul de evaluare aplicat pentru atribuirea contractului:** Prețul cel mai scăzut, per lot, cu corespunderea cerințelor solicitate;

17. **Factorii de evaluare a ofertei celei mai avantajoase din punct de vedere economic, precum și ponderile lor:** Nu se aplică;

Nr.	Denumirea factorului de evaluare	Ponderea%
-	-	-

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

- conform SIA RSAP ;

19. **Adresa la care trebuie transmise ofertele sau cererile de participare:**
Ofertele sau cererile de participare vor fi depuse electronic prin intermediul SIA RSAP
20. **Termenul de valabilitate a ofertelor:** 45 de zile

21. **Locul deschiderii ofertelor:** SIA RSAP

22. **Limba sau limbile în care trebuie redactate ofertele sau cererile de participare:** limba română;

23. **În cadrul procedurii de achiziție publică se va utiliza/accepta:**

Denumirea instrumentului electronic	**Se va utiliza/accepta sau nu**
depunerea electronică a ofertelor sau a cererilor de participare	Se acceptă
sistemul de comenzi electronice	Nu se acceptă
facturarea electronică	Se acceptă
plățile electronice	Se acceptă

24. **Alte informații relevante:** Nu este cazul;

Președintele
grupului de lucru pentru achiziții: Iuri LICHII

Digitally signed by Lichii Iuri
Date: 2024.02.12 11:11:10 EET
Reason: MoldSign Signature
Location: Moldova

Coordonat:

Nr.	**Nume, Prenume**	**Funcția în cadrul grupului de lucru**	**Semnătura**
1.	**Cristina BULIURCĂ**	Membru	Digitally signed by Buliurcă Cristina Date: 2024.02.09 11:31:35 EET Reason: MoldSign Signature Location: Moldova
2.	**Valeria SOROCEAN**	Membru	Digitally signed by Sorocean Valeria Date: 2024.02.09 15:06:29 EET Reason: MoldSign Signature Location: Moldova
3.	**Ghenadie CIUBARA**	Membru	Digitally signed by Ciubara Ghenadie Date: 2024.02.12 09:09:16 EET Reason: MoldSign Signature Location: Moldova
4.	**Sofia CURMEI**	Membru	Digitally signed by Curmei Sofia Date: 2024.02.09 16:59:14 EET Reason: MoldSign Signature Location: Moldova
5.	**Igor ARAMA**	Membru	Digitally signed by Arama Igor Date: 2024.02.09 16:22:15 EET Reason: MoldSign Signature Location: Moldova
6.	**Sergiu CHIRCU**	Membru	Digitally signed by Duca Andrei Date: 2024.02.09 14:42:31 EET Reason: MoldSign Signature Location: Moldova
7.	**Andrei DUCA**	Membru	
8.	**Sergiu BUCIUMAȘ**	Secretar	Digitally signed by Buciumaș Sergiu Date: 2024.02.08 16:28:23 EET Reason: MoldSign Signature Location: Moldova

Digitally signed by Nuța Trofim
Date: 2024.02.08 15:53:08 EET
Reason: MoldSign Signature
Location: Moldova

Digitally signed by Chircu Sergiu
Date: 2024.02.12 11:00:57 EET
Reason: MoldSign Signature
Location: Moldova

Anexa nr. 1
la Anunțul de Participare

Cerințe funcționale față de soluția DLP (Data Loss Prevention)

I. Integrare cu infrastructura IT

1. Soluția trebuie să poată rula pe:
   - Windows 7, 10, 11 Enterprise și Professional, 32-bit sau 64-bit.
   - Windows Server 2022
   - Windows Server 2019
   - Windows Server 2016,
   - Windows Server 2012/2012R2,
   - Windows Server 2008,
   - Linux Ubuntu, CentOS, MacOS
2. Soluția suportă următorul tip directory: Microsoft AD.
3. Soluția trebuie să ofere un mecanism propriu de instalare a agenților pe stațiile de lucru sau alte sisteme conform regulilor configurare și/sau Active Directory (*în continuare* - AD)
4. Soluția trebuie să ofere funcționalități de instalare și deservire de la distanță pentru agenții de monitorizare.
5. Soluția trebuie să ofere suport pentru mediile virtuale:
   - VMware ESXi,
   - ProxMox.
6. Politicile trebuie să se aplice la nivel de user sau stație pe sesiuni multiple.

II. Politici de Securitate

1. Soluția are capacitatea de a inspecta următoarele protocoale:
   - SMTP,
   - Telnet,
   - IMAP,
   - FTP,
   - POP3,
   - IRC,
   - HTTP,
   - HTTPS,
   - SMB,
   - WSD,
   - TCP/IP,
   - LDAP,

   de asemenea poate analiza traficul care este încapsulat în SOCKS;
2. Soluția trebuie să suporte detectarea documentelor înregistrate/amprentate și clasificate.
3. Soluția trebuie să aibă capabilitatea de a proteja datele bazându-se pe punctul lor de origine/creare.

4. Soluția trebuie să fie capabilă să analizeze conținutul și să aplice politici, pentru documentele în limba Română, Rusă, Engleză, Franceză.
5. Soluția trebuie să fie capabila să scaneze și să găsească conținut sensibil.
6. Soluția trebuie să poată proteja informația confidențială care poate fi:
   - scrisă pe unități USB, CD/DVD, carduri SD (inclusiv SDXC și SDHC),
   - trimisă pe mail,
   - upload-ată pe pagini web sau cloud,
   - copiată cu ajutorul clipboard-ului, capturii de ecran (screenshot) a documentelor clasificate,
   - printată în fișier sau pe imprimantă,
   - scrisă pe resursele partajate în rețea,
   - aplicații cloud (DropBox, Google Drive, Box, iCloud, Microsoft OneDrive).
7. Soluția trebuie să poată oferi vizibilitate în timp real a amenințărilor pentru prevenirea pierderilor de date.
8. Soluția trebuie să ofere protecție la nivel de „Clip board" atât pentru copy sau paste cât și pentru screen capture.
9. Soluția trebuie să permită crearea de politici de securitate pentru dispozitivele USB de tip plug-and-play.
10. Soluția trebuie să ofere același nivel de protecție și în regim OS Safe-Mode.
11. Soluția trebuie să fie capabilă să facă analiză de conținut local (offline), fără a utiliza vreo altă componentă a soluției.
12. Soluția permite auditarea funcționalității agentului de endpoint.
13. Soluția trebuie să aibă un mecanism propriu de instalare a agenților pe stațiile de lucru sau alte sisteme.
14. Agentul de endpoint trebuie să fie compatibil, cu soluții de antivirus, firewall și antispyware third-party (de ex: Kaspersky, BitDefender, McAfee, Norton, Safeguard, Acronis, Spybot, Adaware).
15. Soluția trebuie să permită realizarea unui proces de justificare, în cazul în care utilizatorul transmite conținut confidențial.
16. Opțiunea de justificare a activității folosită de end-user în cadrul procesului de justificare, trebuie să poată fi validabilă sau administrabilă.
17. Soluția trebuie să fie capabilă să blocheze dispozitivele portabile sau să permită doar accesul de tip read-only.
18. Soluția trebuie să poată aplica reguli de protecție care să aibă ca criteriu cuvinte-cheie, expresii regulate și amprentă (hash-uri).
19. Construcția regulilor trebuie să includă suport pentru logica booleana incluzând AND, OR, sau alte declarații logice.
20. Soluția trebuie să fie capabilă să aplice următoarele acțiuni: blocare, monitorizare, notificare utilizator, menținere evidentă, criptare.
21. Posibilitatea notificării utilizatorilor cu privire la încălcarea confidențialității documentelor procesate (notificare prin e-mail, push-notificare, etc.).
22. Soluția trebuie să aibă abilitatea de a identifica fișierele bazându-se pe conceptul de true file type și nu doar pe extensia fișierelor.
23. Soluția trebuie să aibă posibilitatea rulării autonome a agentului pe endpoint în baza politicilor inițial aplicate.
24. Soluția trebuie să fie capabilă să aplice reguli de protecție atât la nivel de grupuri /user-i definiți în Active Directory cât și pentru user-ii locali ai sistemelor.

25. Soluția trebuie să fie capabilă să aplice reguli de control al perifericelor chiar și atunci când nu este conectat la rețeaua companiei, cu posibilitatea de a avea politici diferite în funcție de conectivitatea la rețeaua companiei.
26. Soluția trebuie să dețină posibilitatea de generare a rapoartelor predefinite și expedierea acestora pe e-mail.
27. Soluția are abilitatea de a face discovery în interiorul bazelor de e-mail stocate pe endpoint.
28. Soluția trebuie să permită customizarea notificărilor emise în timpul funcționării și a ferestrei în care sunt scrise aceste notificări.
29. Soluția trebuie să fie capabilă să identifice nivelul de clasificare a documentelor din marcajele vizuale și să aplice regulile de protecție pe aceste documente.
30. Soluția trebuie să fie capabilă să protejeze documente nemarcate ce au conținut ce provine din documente clasificate cu marcaje vizuale.
31. Soluția trebuie să aibă opțiunea de clasificare a datelor sau integrarea cu alte produse de clasificare a datelor.
32. Soluția trebuie să poată aplica etichete fișierelor în funcție de originea lor, informația fiind stocată securizat pentru a nu putea fi alterată de utilizator.
33. Soluția trebuie să fie capabilă să citească informațiile de tip META stocate în fișierele Office.
34. Soluția trebuie să ofere utilizatorilor capabilități de clasificare manuala a email-ului la momentul trimiterii unui e-mail folosind clientul Outlook office.
35. Politicile atribuite utilizatorilor/grupelor de utilizatori să se aplice momentan, sau să se dețină un mecanism care ar aplica forțat aceste politici/reguli pe stația de lucru.
36. Posibilitatea de efectuare a copiilor de rezervă (back-up) pentru incidentele înregistrate pentru o perioadă anumită (stabilită de către administrator) și pentru întregul volum de date.
37. Posibilitatea de eliberare a informațiilor neutilizate/istorice din baza de date.
38. Posibilitatea descărcării fișierelor din mai multe incidente înregistrate pe un utilizator (în mod automat).
39. Posibilitatea de adăugare a aplicațiilor de pe PC pentru monitorizare în consola DLP.
40. Clasificarea regulilor/politicilor individuale pentru aplicații în parte, precum și aplicarea multiplă a seturilor de reguli.
41. Sistemul trebuie să ofere un mecanism de rezolvare a conflictelor dintre reguli pentru a evita inconsecvențele în aplicarea acestora.
42. Posibilitatea de adăugare a utilizatorilor în excepții pentru toate politicile în ansamblu, în acest caz monitorizarea evenimentelor utilizatorilor vor fi monitorizate fără aplicarea restricțiilor.
43. Posibilitatea de presetare a posibilității de amânare a excepțiilor în mod automat sau la un timp prestabilit de către administrator.
44. Soluția trebuie să ofere politici de securitate out-of-box care pot fi constumizate de către utilizator.
45. Soluția trebuie să ofere posibilitatea clasificării în timp real pentru a minimiza false pozitive.
46. Soluția trebuie să permite protejarea stațiilor de lucru mobile care sunt/nu sunt conectate la rețea.

III. Consola de administrare

1. Consola de administrare trebuie sa se poată instala pe unul din următoarele sisteme de operare pe 64 de biți:
   - Microsoft Windows Sever 2016,
   - Microsoft Windows Sever 2012 Release 2 (R2),
   - Microsoft Windows Server 2012.
2. Soluția trebuie să permită instalarea/dezinstalarea agentului în mod centralizat.
3. Consola trebuie să permită pe lângă distribuirea componentelor native și împachetarea aplicațiilor de la terți și instalarea acestora pe stațiile de lucru.

4. 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).
5. Consola de administrare trebuie să poată fi integrată cu Active Directory.
6. Consola de administrare trebuie să poată fi instalată într-un mediu virtual.
7. Consola de administrare trebuie să utilizeze bază de date freeware sau licența soluției să cuprindă și licența bazei de date utilizate.
8. Consola de administrare permite instalarea unei componente de comunicare în DMZ pentru a putea permite sincronizarea sistemelor prin internet.
9. Acces-ul în consola de administrare să poată fi făcut pe baza credențialelor din Active Directory.
10. Consola de administrare trebuie să permită crearea de roluri în mod granular pentru cei ce o administrează.
11. Toate acțiunile utilizatorilor în consola de administrare trebuie auditate.
12. Consola trebuie să permită construirea unei liste de contacte în vederea folosirii acestora pentru notificări prin mesagerie electronica (E-mail).
13. Canalul de comunicație dintre serverul de administrare si componentele distribuite pe calculatoare trebuie sa fie criptat.
14. Componența ce asigură canalul de comunicație dintre server și stații de lucru trebuie să fie văitată din punct de vedere al securității. (Ex: FIPS, Common Criteria, Etc.)
15. Canalul de comunicație dintre consola și cei ce o accesează trebuie să fie criptat.
16. Consola de administrare trebuie să poată fi accesată de pe orice computer din rețea în mod Web securizat utilizând un browser standard (Internet Explorer, Chrome, Firefox), fără necesitatea instalării de software adițional.
17. Intervalul de transmitere a evenimentelor de pe client către server poate fi modificat.
18. Consola trebuie să poată detecta prezenta pe rețea a sistemelor noi apărute prin intermediul unor senzori.
19. Consola trebuie să folosească un propriu index pentru a identifica și actualiza datele despre sistemele care își schimbă proprietăți precum nume, IP și configurații hardware;
20. Consola permite automatizarea de sarcini de instalare/dezinstalare a componentelor pe stațiile de lucru, de rulare a rapoartelor și de transmiterea de notificări prin mesagerie electronica.
21. Consola trebuie să prezinte cel puțin următoarele informații despre sistemele administrate: numele sistemului, utilizatorul logat, produsele instalate, tipul de system de operare și adresa IP.
22. Serverul de administrare 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 în rețea).
23. Consola trebuie sa permite aplicarea de politici diferite pentru sisteme pe:
    - Sisteme individuale,
    - Grupuri de sisteme,
    - Sisteme din AD ce sunt același OU.
24. Consola trebuie să știe să lanseze automat aplicații externe și să injecteze parametrii din evenimente.
25. Consola trebuie să permită accesarea log-ului componentei de sincronizare de pe sisteme în timp real prin intermediul unui serviciu web.
26. Consola trebuie să permită vizualizarea incidentelor de securitate și crearea de cazuri.
27. Consola trebuie să permită integrarea și altor aplicații/echipamente de securitate ex. (Antivirus, SandBox, Proxy, Firewall) într-o consola unica pentru a unifica administrarea acestora.

IV. Raportarea

1. Consola de administrare trebuie să asigura generarea de rapoarte despre nodurile administrate și despre evenimentele generate de ele.
2. Consola trebuie să permită crearea de noi rapoarte în mod granular cu informații extrase din evenimente, sau despre sistemele administrate.
3. Consola trebuie să includă posibilitatea de generare a rapoartelor precum: număr incidente pe sistem/utilizator, istoria utilizatorilor autentificați în sistem, integrarea grupelor de utilizatori din AD.
4. Rapoartele trebuie să fie generate sub forma de tabel, lista, sumar, sau grafic istoric.
5. Rapoartele trebuie să poată să fie exportate în format pdf, csv, html.
6. Rapoartele trebuie să poată să fie salvate ca fișiere sau trimise prin e-mail.
7. Rapoartele trebuie să poată să fie exportate într-un format arhivat și expediate automat pe e-mail unor destinații presetate.
8. Consola trebuie să permită să evalueze evenimentele primite de la stațiile de lucru și filtrarea lor pentru o mai buna identificare a informațiilor relevante.
9. Să se poată genera rapoarte utilizând:
    - Log-ul de audit administrativ,
    - Detalii despre sistemele administrate (detalii de configurare, hardware, utilizator),
    - Evenimente de sisteme,
    - Informații despre politicile și sarcinile aplicate sistemelor,
    - Informații furnizate de senzori.

V. Solicitări suplimentare

1. Oferta trebuie să acopere 100 de stații de lucru.
2. Ofertantul trebuie să posede oficiu de suport local, iar timpul de suport să fie 8/24 ore și 5/7 zile.
3. Oferta trebuie să includă și serviciile de instalare și configurare.
4. Ofertantul trebuie să fie partener oficial al furnizorului de servicii DLP.
5. Ofertantul trebuie să aibă în state minim doi specialiști tehnici certificați pe produsul propus.
6. Ofertantul la solicitarea cumpărătorului (după necesitate) să fie pregătit pentru a prezenta funcționalitățile produsului instalat, pe o platformă de testare, înainte de scurgerea timpului de anunțare a învingătorului.
7. Oferta să conțină costul utilizării soluției pentru un an calendaristic și nelimitat (dacă există acest tip de licență).
8. În dependență tipul licenței achiziționate (anuală sau pentru totdeauna), suportul trebuie să fie inclus în oferta de preț.