ANUNŢ DE PARTICIPARE SIMPLIFICAT
PENTRU ACHIZIŢIA DE VALOARE MICĂ (04.10.2023)

Privind achiziţionarea: **Echipamentului Fortinet Fortigate 201F sau echivalentul, prin achiziţie publică de valoare mică.**

1. Denumirea autorităţii contractante: **Agenția de Stat pentru Proprietatea Intelectuală (AGEPI).**
2. IDNO **1015601000112.**
3. Adresa: **MD-2024, _mun. Chişinău, str. Andrei Doga 24/1.**
4. Numărul de telefon/fax: **022 188627; 022 188688; 022 188570/022 188699**
5. Adresa de e-mail şi pagina web oficială ale autorităţii contractante: ***office@agepi.gov.md; tender@agepi.gov.md; www.agepi.gov.md.***
6. Adresa de e-mail sau pagina web oficială de la care se va putea obţine accesul la documentaţia de atribuire: **documentația de atribuire este anexată în cadrul procedurii în SIA RSAP, și/sau la link-ul https://agepi.gov.md/ro/content/achizi%C5%A3ii .**
7. Tipul autorităţii contractante şi obiectul principal de activitate (dacă este cazul, menţiunea că autoritatea contractantă este o autoritate centrală de achiziţie sau că achiziţia implică o altă formă de achiziţie comună): **Autoritate Administrativă Centrală în subordinea Guvernului, responsabilă de promovarea și realizarea activităților în domeniul protecției juridice a proprietății intelectuale privind drepturile de proprietate industrială, dreptul de autor și drepturile conexe.**
8. Cumpărătorul invită operatorii economici interesaţi, care îi pot satisface necesităţile, să participe la procedura de achiziţie privind livrarea/prestarea următoarelor bunuri/servicii:

Nr. crt.	Codul CPV	Denumirea bunurilor/serviciilor	Unitatea de măsură	Canti-tatea	Specificarea tehnică deplină solicitată, standardele de referinţă
Echipament Fortinet Fortigate 201F sau echivalentul					
1	32420000-3	**Echipament Fortinet Fortigate 201F sau echivalentul**	Buc.	1	**Tip: Echipament integrat de protecție a rețelei ce funcționează ca o soluție de securitate unificat**ă, inclusiv 12 luni de suport și subscriere de la producător. Cantitatea și cerințe de licențiere: - Este responsabilitatea Ofertantului de a determina modelul de licențiere și cantitatea licențelor. - Toate licențele livrate vor include prețul pentru 12 luni de suport și subscriere furnizat de producătorul licențelor, care va începe de la data acceptanței soluției, după instalare și testare a funcționalităților. În cazul activării licențelor până la data acceptanței soluției, toate costurile de licențiere de la producător în perioada de până la acceptanță vor fi suportate de către Ofertant (Furnizor). **Cerințe tehnice:** Soluția propusă trebuie sa fie o soluție inovatoare, care va asigura următoarele cerințe minime: **1.** Specificații hard.ware: • Interfețe GbE RJ-45: 16 • Interfețe management/HA/DMZ GbE RJ-45: 1/2/1 • Interfete WAN Gbe RJ-45: 2 • Interfete combo RJ45/SFP Gbe: 4 • Sloturi GE SFP: 8 • Sloturi 10GE SFP+: 2 • Porturi consola RJ-45: 1 • Porturi USB: 1 • Dimensiune: 1U • Alimentare redundantă • Stocare interna SSD: 1x 480 GB SSD. **2. Caracteristici:** • Trafic firewall (1518/512/64 byte pachete UDP): 27/27/11 Gbps • Latenta Firewall: 4.78 µs • Trafic Firewall măsurat în pachete per secunda: 15 Mpps

Nr. crt.	Codul CPV	Denumirea bunurilor/serviciilor	Unitatea de măsură	Canti-tatea	Specificarea tehnică deplină solicitată, standardele de referinţă
Echipament Fortinet Fortigate 201F sau echivalentul					
					• Trafic IPSec VPN (512 byte packets): 13 Gbps • Trafic IPS: 5 Gbps • Trafic NGFW: 3.5 Gbps • Performanta SSL Inspection (IPS, HTTP): 3 Gbps • Număr de tunele IPSec VPN site-to-site: 2.000 • Număr de clienți IPSec VPN: 16.000 • Trafic SSL-VPN: 4 Gbps • Număr de clienți concurenți SSL-VPN: 500 • Număr de sesiuni concurente TCP: 3.000.000 • Număr de sesiuni noi pe secundă TCP: 280.000 • Număr de politici de securitate: 10.000 • Număr de instanțe virtuale: 10 • Număr de AP-uri administrate (total/tunnel mode): 256/128 • Trafic CAPWAP: 20 Gbps • Număr de token-uri OTP administrate: 5.000. **3. Funcționalități generale:** • Filtru de SPAM și viruși; Echipament integrat de securitate cu funcționalități simultane de: - Firewall de tip stateful - Router cu suport pentru protocoale de rutare dinamice - Posibilitate de instalare în mod bridge Ethernet - Protecție Antivirus - Criptare de date: IPSec VPN si SSL VPN - Suport pentru QoS si Traffic Shaping - Detecția si prevenirea intruziunilor – IDS/IPS - Scanare si filtrare WEB – Web Inspection/Filter - Blocarea si controlul traficului din rețea generat de aplicații - Protecție Antispam - Protecție împotriva scurgerii de informații confidențiale - Update-uri automate și în timp real - Suport pentru IPv6 UTM - Funcționalitate de proxy SSL – posibilitatea inspecției traficului criptat - Wireless controller • Toate funcționalitățile de securitate (antivirus, IPS, antispam, Web filtering), tehnologiile incluse, sistemul de operare precum și platforma hardware aparțin aceluiași producător • Echipamentul firewall trebuie sa asigure management pentru Switch/ Acces Point • Certificări pentru producător și produs: ICSA Labs pentru Firewall, IPSec, SSL VPN, IPS, Antivirus • Conformitate cu: CE, CB. **Funcționalități securitate:** **4. Funcționalități firewall:** • Funcționalități NAT, PAT și Transparent Bridge • Opțiune de a aplica NAT per politica • Suport VLAN Tagging 802.1Q • Autentificarea utilizatorilor pe grupuri • Suport VoIP SIP/H.323/SCCP Traversal NAT • Funcționalitate proxy explicit HTTP/HTTPS și FTP • Suport pentru proxy chaining cu balansare de sesiuni prin proxy-uri multiple pentru funcționalitatea proxy explicit • Suport WINS

Nr. crt.	Codul CPV	Denumirea bunurilor/serviciilor	Unitatea de măsură	Canti-tatea	Specificarea tehnică deplină solicitată, standardele de referinţă
Echipament Fortinet Fortigate 201F sau echivalentul					
					• Suport securitate VoIP ALG (SIP Firewall/RTP Pinholing) • Suport pentru TCP MSS clamping • Suport pentru rescrierea câmpului Class of Service • Suport IPv6 (NAT/mod Transparent) • Politici de securitate bazate pe identitatea utilizatorului/servicii folosite/tipul device-ului sau al sistemului de operare de stație folosit – funcționalitate de tip BYOD (bring your own device) • Opțiune "Scheduling" pentru politicile de firewall • Posibilitate de blocare a traficului după tara de origine a sursei sau destinației (Geo IP) • Mecanism de calcul și afișare al reputației utilizatorilor din rețea pe baza de scor dedus în mod configurabil din activitatea detectata prin mecanismele de inspecție de blocarea a atacurilor, blocare malware, filtrare web, firewall și inspecție a traficului de aplicații. **5. Funcționalități VPN:** • Suport PPTP, L2TP, IPSec, L2TP over IPSec, SSL-VPN • Criptare DES, 3DES, AES 128, AES 192, AES 256 • Autentificare MD5, SHA-1, SHA-256, SHA-384, SHA-512 • Suport pentru PPTP și L2TP VPN Client Pass Through • Funcționalitate "Hub and Spoke" IPSec VPN • Autentificare IKE prin certificate X.509 - suport pentru RSA și ECDSA • Suport IPSec Xauth NAT Traversal • Suport configurare IPSec automata • Funcționalitate IKE Dead Peer Detection • Suport pentru RSA SecureID • Suport Single-Sign-On pentru book-mark-uri portal SSL-VPN • Funcționalitate Two-Factor Authentication pentru SSL-VPN • Suport pentru autentificare de grupuri de utilizatori prin LDAP (SSL-VPN) • Suport tunele SSL în mod tunel și în mod portal • Suport pentru validarea clienților SSL VPN prin verificarea aplicațiilor instalate pe stație înainte de conectare - compatibilitate cu sistemele de operare Windows • Suport pentru limitarea aplicațiilor utilizabile pe stațiile clienților SSL VPN după conectare - compatibilitate cu sistemele de operare Windows • Suport pentru izolarea datelor utilizate în cadrul sesiunii SSL VPN de restul aplicațiilor ce rulează pe stațiile utilizatorilor și ștergerea acestora după terminarea sesiunii SSL VPN - compatibilitate cu sistemele de operare Windows • Suport pentru autentificarea utilizatorilor de tip Single Sign On prin portalul SSL VPN • Funcționalități monitorizare tunele VPN. **6. Funcționalități Antivirus:** • Filtru de SPAM și viruși; Protecție anti-malware (virus, troian, worm, spyware, grayware) • Protocoale suportate: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S IMAP/IMAPS, MAPI, FTP • Suport scanare antivirus Proxy-Based și Flow-Based • Opțiune pentru detecția malware prin sandboxing de tip Cloud-Based al fișierelor suspecte, oferita de producător • Update-uri automate de semnături malware

Nr. crt.	Codul CPV	Denumirea bunurilor/serviciilor	Unitatea de măsură	Canti-tatea	Specificarea tehnică deplină solicitată, standardele de referinţă
Echipament Fortinet Fortigate 201F sau echivalentul					
					• Protecție împotriva rețelelor botnet și site-urilor de tip phishing pe baza de reputație a adreselor IP și a URL-urilor accesate de utilizatori. **7. Funcționalități filtrare trafic WEB:** • Filtrare pentru protocoalele HTTP si HTTPS • Filtrare după categorii site-uri/URL-uri • Funcționalitate de contorizare a timpului de acces sau a volumului de trafic pentru utilizatori – definire de cote de utilizare • Blocare a conexiunilor în funcție de URL/cuvânt cheie sau expresie în conținutul paginilor web • Blocare a conexiunilor în funcție de URL-ul din header-ul Referer al cererii HTTP • Filtrare pentru Java Applet, Cookies, scripturi Active X • Posibilitate de activare forțată a opțiunii „Safe Search" pentru motoare de căutare web • Posibilitatea de modificare a header-elor HTTP din cererile generate de utilizatori • Funcționalitate de monitorizare a activității web a utilizatorilor • Posibilitate de înștiințare a utilizatorilor, prin afișarea informațiilor în cadrul unui browser web, privind paginile web blocate. **8. Funcționalități sistem de control al aplicațiilor**: • Identificarea și controlul a peste 3000 de aplicații • Opțiune de Traffic-Shaping per aplicație • Control specific pentru aplicațiile de tip IM/P2P • Clasificare granulara a aplicațiilor după criterii multiple precum: Categorii de aplicații, Popularitate, Tehnologie și Risc • Monitorizare aplicațiilor cu rata cea mai mare de consum de banda • Monitorizarea aplicațiilor pe baza IP/Utilizator • Suport pentru decriptarea și inspectarea sesiunilor SSH • Suport pentru blocarea aplicațiilor utilizate în cadrul rețelelor de tip Botnet • Posibilitate de definire a semnăturilor de aplicație personalizate • Posibilitate de înștiințare a utilizatorilor, prin afișarea informațiilor în cadrul unui browser web, privind traficul de aplicații blocat. **9. Funcționalități sistem de prevenire a intruziunilor/atacurilor (IPS):** • Protecție pentru peste 10.000 de semnături de atac • Suport pentru inspecția traficului de aplicație criptat prin protocolul SSL • Protecție pentru atacuri de tip brute force • Detectarea anomaliilor de protocol • Suport pentru semnături configurabile • Update-uri automate pentru semnături • Suport pentru IPv4 și IPv6 DoS/DDoS. **10. Funcționalități Antispam:** • Scanare pentru SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI • Suport RBL/ORDBL • Inspecție header MIME • Filtrare după cuvinte cheie/expresie • Filtrare după Black/White List pentru adrese IP și e-mail • Update-uri automate și în timp real. **11. Funcționalitate Data Leak Prevention:**

Nr. crt.	Codul CPV	Denumirea bunurilor/serviciilor	Unitatea de măsură	Canti-tatea	Specificarea tehnică deplină solicitată, standardele de referinţă
Echipament Fortinet Fortigate 201F sau echivalentul					
					• In caz de scurgere de informații trebuie sa permită blocarea și arhivarea conversației pe protocoale de email, HTTP, FTP și variantele criptate SSL; • Blocare după tip și dimensiune fișier • DLP fingerprint și arhivare. **12. <u>Funcționalități sistem de verificare a stațiilor (Endpoint Control):</u>** • Integrare cu o aplicație software pentru securitate ce rulează pe stații care sa permită: - Blocarea traficului de aplicații instalate pe stații - Restricționarea/filtrarea accesului web - Scanarea pentru vulnerabilități a stațiilor - Scanare Antivirus - Configurarea automata pentru tunele VPN. **Funcționalități rețea:** **13. <u>Funcționalități rețea și rutare:</u>** • SD-WAN-control inteligent al interfeței WAN, prin direcționarea traficului prin aceasta având link-uri configurate care pot susține peste 5000 de aplicații și utilizatori/grupuri de utilizatori. Suport pentru legături WAN multiple cu balansare a traficului după metodele: - Weighted round robin a sesiunilor, împărțire proporțională a volumului de trafic, prin limitarea per interfață a benzii maxime utilizabile, după calitatea conexiunii ISP (jitter sau latenta). • Suport PPPoE și DHCP Client/Server • Rute statice • Rutare dinamica IPv4: RIP, OSPF, BGP, Multicast (PIM–DM, PIM–SM, IGMP v1 v2 v3), IS-IS • Rutare dinamica IPv6: RIPng, OSPF v3, BGP 4+ • Gruparea interfețelor în zone de securitate • Rutare intre zonele de securitate • Policy-based routing • Suport VRRP și Link Failure Control • Suport VLAN Tagging (802.1q) • Rutare intre VLAN-uri • Suport pentru IPv6 (Firewall, DNS, SIP) • Posibilitate mapare (Binding) adrese IP – adrese MAC • Suport One-to-One NAT • Tunelare IP în IP • Suport NAT64, DNS64, NAT46, NAT66 • Suport LLDP. **14. <u>Funcționalitate Wireless Controller:</u>** • Modul wireless controller pentru thin-AP-uri integrat cu următoarele funcționalități: - Detecție și suprimare a AP-urilor neînregistrate în controller; - Selecție automata a canalului pentru AP în funcție de interferentele din mediu; - Suport pentru SSID-uri multiple; - Autentificare WEP, WPA, WPA2, WPA2 Enterprise, 802.1x - Suport Captive Portal; - Funcționalitate de gestionare a conturilor de tip guest prin intermediul unei interfețe web diferita de interfața pentru administrare globala; - Suport pentru Wireless Mesh si roaming; - Distribuire automata a clienților wireless per AP sau banda de frecvente pentru a obține performante optime.

Nr. crt.	Codul CPV	Denumirea bunurilor/serviciilor	Unitatea de măsură	Canti-tatea	Specificarea tehnică deplină solicitată, standardele de referinţă
Echipament Fortinet Fortigate 201F sau echivalentul					
					- Rutare dinamica a traficului generat de utilizatorii wireless prin VLAN-uri folosind autentificare prin RADIUS - Autentificare suplimentara a clienților wireless prin RADIUS pe baza adresei MAC - Suport pentru RADIUS Accounting - Posibilitatea gestionarii AP-urilor remote de către controller dar cu rutarea traficului printr-un gateway local - Wireless IDS - Monitorizarea activa a utilizării spectrului de frecvente radio. **15. Funcționalități Traffic Shaping:** • Limitare/garantare/prioritizare a benzii de trafic prin politici • Traffic Shaping per aplicație și adresa IP • Suport pentru DSCP • Limitare a cotei de trafic (per adresa IP) • Suport pentru ToS. **16. Funcționalități High Availability - HA:** • Funcționare Active-Active, Active-Passive • Funcționalitate Stateful Failover (Firewall si VPN) • Detectare și notificare pentru echipament nefuncțional • Monitorizarea conexiunii la rețea • Funcționalitate Link Failover. **Funcționalități de administrare, logare, autentificare a utilizatorilor:** **17. Funcționalități de administrare:** • Administrare prin WEB UI, Secure Command Shell (SSH) si Command Line Interface (CLI) • Posibilitatea de administrare dintr-un portal cloud-based oferit de producător • Utilizatori/Administratori cu drepturi configurabile • Funcționalitate de export/import a configurației • Politica de control a parolelor. **18. Funcționalități de logare și monitorizare:** • Opțiune de păstrare a log-urilor pe memoria internă. **19. Funcționalități de autentificare a utilizatorilor:** • Definire locala a utilizatorilor • Integrare cu Windows Active Directory (AD) pentru Single Sign On • Integrare cu Citrix pentru autentificare SSO a utilizatorilor • Integrare cu RADIUS/LDAP/TACACS+/POP3 • Suport Xauth pentru IPSec VPN • Suport pentru autentificarea grupurilor de utilizatori prin LDAP • Suport pentru autentificare prin doi factori folosind OTP generate de token-uri fizice sau software ce pot fi trimise utilizatorilor prin Email sau SMS • Suport pentru autentificare prin certificate digitale PKI X.509 • Posibilitatea limitării accesului utilizatorilor în rețea ce nu au instalat un client software de stație (client endpoint). **20. Condiții de alimentare:** • Alimentare curent alternativ 100-240V, 50-60 Hz • Consum maxim de putere: 121.94 W. **21. Condiții de mediu:** • Temperatura de operare: 0 – 40 grade Celsius • Umiditate: 10–90 %, fără condens. **22. Garanție si suport:**

Nr. crt.	Codul CPV	Denumirea bunurilor/serviciilor	Unitatea de măsură	Canti-tatea	Specificarea tehnică deplină solicitată, standardele de referinţă
Echipament Fortinet Fortigate 201F sau echivalentul					
					• Solutia va beneficia **de minimum un an** ce va include: • Înlocuirea echipamentului în caz de defecțiune hardware • Suport tehnic din partea producătorului 7 zile pe săptămâna, 24 de ore pe zi, în regim Next Business Day • Update firmware versiuni minore și majore • Soluția va beneficia de update-uri automate de semnături de securitate pentru îndeplinirea funcționalităților de Antivirus, Web Filtering, Antispam, Application Control și IPS timp de minimum trei ani. **Alte cerințe obligatorii**: Costul ofertei trebuie să includă activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției. **În echipament trebuie sa fie prezent un controler Wi-Fi integrat și compatibil cu următoarele echipamente, care fac parte din rețeaua Wi-Fi a agenției: 1. FortiAP14C; 2. FortiAP21D; 3. FortiAP24D**
Valoarea estimativă totală					**258 333,00 lei fără TVA**

9. În cazul în care contractul este împărţit pe loturi, un operator economic poate depune oferta (se va selecta): **Nu este împărțit pe loturi. Este un singur lot**.

10. Termenele şi condiţiile de livrare/prestare solicitate: **În termen de 60 zile din data intrării în vigoare a contractului (data înregistrării contractului la una din Trezoreriile Regionale ale Ministerului Finanţelor). Livrare, instalare gratuită la sediul AGEPI.**

11. Termenul de valabilitate a contractului **31.12.2023.**

12. Scurtă descriere (indicaţi după caz) a criteriilor de calificare:

Nr. crt.	Criteriile de calificare şi de selecţie (descrierea criteriului/cerinţei)	Modul de demonstrare a îndeplinirii criteriului/cerinţei	Nivelul minim/ obligativitatea
1.	Specificații tehnice (anexa nr. 22 la Documentația standard pentru realizarea achizițiilor publice de bunuri și servicii, aprobată prin Ordinul Ministrului Finanțelor nr. 115 din 15.09.2021 (în continuare Documentația standard))	Original autentificat prin semnătura electronică a ofertantului	Obligatoriu
2.	Specificații de preț (anexa nr. 23 la Documentația standard)	Original autentificat prin semnătura electronică a ofertantului	Obligatoriu
3.	Certificat/decizie de înregistrare a întreprinderii, Extras din Registrul de Stat al Unităţilor de drept	Copie autentificată prin semnătura electronică a ofertantului	Obligatoriu
4.	Certificat privind lipsa sau existența restanțelor față de BPN	Copie autentificată prin semnătura electronică a ofertantului	Obligatoriu
5.	Certificat de atribuire a contului bancar	Copie autentificată prin semnătura electronică a ofertantului	Obligatoriu
6.	Declarație de eligibilitate completată în conformitate cu pct. 52 din Regulamentului cu privire la achizițiile publice de valoare mică, aprobat prin Hotărârea Guvernului nr. 870/2022 (anexa nr. 2 la Regulament)	Original autentificat prin semnătura electronică a ofertantului	Obligatoriu
7.	Actul care atestă dreptul de a livra bunuri//servicii	Copia autorizației de la producător (dovada deținerii statutului de Distribuitor sau Partener oficial al producătorului) care confirmă dreptul Ofertantului de a livra echipamentul propus, autentificată prin semnătura electronică a ofertantului	Obligatoriu
8.	Declarație prin care se confirmă că producătorul de echipamente electrice și electronice (EEE) este inclus în Lista producătorilor de produse supuse reglementărilor	Copie autentificată prin semnătura electronică a ofertantului	Obligatoriu

Nr. crt.	Criteriile de calificare şi de selecţie (descrierea criteriului/cerinţei)	Modul de demonstrare a îndeplinirii criteriului/cerinţei	Nivelul minim/ obligativitatea
	de responsabilitate extinsă a producătorilor, în condițiile pct. 111 din Regulamentul privind deșeurile de echipamente electrice și electronice, aprobat prin HG nr. 212/2018		
9.	Confirmare privind înregistrarea în „Lista producătorilor" de produse supuse reglementărilor de responsabilitate extinsă a producătorilor (baterii și acumulatori) în condițiile Regulamentului privind gestionarea bateriilor şi acumulatorilor şi deşeurilor de baterii şi acumulatori, aprobat prin HG nr. 586/2020	Copie – autentificată prin semnătura electronică a ofertantului.	Obligatoriu
10.	Dovada deținerii Centrului autorizat de deservire tehnică a echipamentului ofertat, cu specialiști calificați, cu indicarea condițiilor de menținere și suport pentru perioada de garanție	Copie autentificată prin semnătura electronică a ofertantului	Obligatoriu
11.	Declarație privind personalul de specialitate propus pentru implementarea contractului (anexa nr. 14 la Documentația standard)	Declarație autentificată prin semnătura electronică a ofertantului (cu anexarea documentelor corespunzătoare: Certificate, CV-uri)	Obligatoriu
12.	Declarație privind lista principalelor livrări/prestări efectuate în ultimii 3 ani de activitate (anexa nr. 12 la Documentația standard)	Declarație autentificată prin semnătura electronică a ofertantului	Obligatoriu
13.	Certificate sau alte documente emise de organisme abilitate în acest sens, care să ateste conformitatea echipamentului	Copie autentificată prin semnătura electronică a ofertantului	Obligatoriu
14.	Demonstrarea certificării a operatorului economic cu standardele ISO 27001/ 9001	Copie autentificată prin semnătura electronică a ofertantului	Obligatoriu

13. Tehnici şi instrumente specifice de atribuire (după caz, specificaţi dacă se va utiliza licitaţia electronică): **Nu se aplică.**

14. Condiţii speciale de care depinde îndeplinirea contractului (indicaţi după caz): **Costul ofertei trebuie să includă activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției. În echipament trebuie sa fie prezent un controler Wi-Fi integrat și compatibil cu următoarele echipamente, care fac parte din rețeaua Wi-Fi a agenției: 1. FortiAP14C; 2. FortiAP21D;3. FortiAP24D.**

15. Ofertele se prezintă în valută: **Nu se aplică.**

16. Criteriul de evaluare aplicat pentru atribuirea contractului: **Prețul cel mai scăzut și corespunderea specificațiilor tehnice.**

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

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: **60 de zile.**

21. Locul deschiderii ofertelor: **SIA „RSAP". *Ofertele întârziate vor fi respinse*.**

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

23. Alte informații relevante: -

Președinte al grupului de lucru
în domeniul achizițiilor publice în cadrul AGEPI: _____ Vadim URSU

Digitally signed by Ursu Vadim
Date: 2023.10.04 15:51:29 EEST
Reason: MoldSign Signature
Location: Moldova