MUNICIPIUL CRAIOVA
PRIMĂRIA MUNICIPIULUI CRAIOVA
DIRECŢIA R.P.M.D.
SERVICIUL M.D.I.P.
COMPARTIMENTUL INFORMATICĂ
Nr. 256317/16 .07.2024

CAIET DE SARCINI

pentru achiziţie tehnică de calcul – Routere/firewall de mare viteza, storage-uri de rețea și surse rackabile UPS 3000VA

1 Introducere

Caietul de sarcini face parte integrantă din documentația de atribuire și constituie ansamblul cerințelor pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică.

Toate cerinţele din prezentul Caiet de Sarcini sunt minimale şi obligatorii. Specificațiile tehnice care indică o anumită origine, sursă, producție, un procedeu special, o marcă de fabrică sau de comerț, un brevet de invenție, o licență de fabricație, sunt menționate doar pentru identificarea cu ușurință a caracteristicilor produsului și nu au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificații vor fi considerate ca având mențiunea de «sau echivalent» iar ofertantul are obligația de a demonstra echivalența produselor ofertate cu cele solicitate sau –după caz- superioritatea lor tehnică. În acest sens, orice ofertă prezentată, care se abate de la prevederile Caietului de sarcini, va fi luată în considerare, numai în măsura în care propunerea tehnică presupune asigurarea unui nivel calitativ superior cerințelor minimale din Caietul de sarcini. Ofertele care nu satisfac cerințele caietului de sarcini vor fi declarate neconforme și vor fi respinse.În cadrul acestei proceduri, Municipiul Craiova îndeplinește rolul de Autoritatea/entitatea contractantă, respectiv Autoritatea/entitatea contractantă în cadrul Contractului.

Pentru scopul prezentei secțiuni a Documentației de Atribuire, orice activitate descrisă într-un anumit capitol din Caietul de Sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către Ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului Contractului.

2 Contextul realizării acestei achiziții de produse

Obiectul acestui contract este procurarea și livrarea echipamentelor IT si a software-ului necesar funcţionării acestora, asa cum sunt ele descrise mai jos

2.1 Informații despre Autoritatea/entitatea contractantă

Autoritatea Contractantă: MUNICIPIUL CRAIOVA, JUDEȚUL DOLJ

Date de contact: Municipiul Craiova, Craiova, județul Dolj, strada Târgului, nr.26 – Centru Multifuncțional.

Localitatea: Craiova, Cod poștal: 200632, Romania, Tel. +40 0251416235, Fax: +40 0251415907

Email: achizitii@primariacraiova.ro, , Adresa internet (URL): www.primariacraiova.ro,

Adresa profilului cumpărătorului (URL): www.e-licitatie

2.2 Informații despre contextul care a determinat achiziționarea produselor

În vederea desfășurării în condiții optime și eficientizarea activității compartimentelor din cadrul Primăriei Municipiului Craiova.

2.3 Informații despre beneficiile anticipate de către Autoritatea/entitatea contractantă

Scurtarea timpilor de procesare a informațiilor.

2.4 Alte inițiative/proiecte/programe asociate cu această achiziție de produse, dacă este cazul

Nu este cazul

2.5 Cadrul general al sectorului în care Autoritatea/entitatea contractantă își desfășoară activitatea

Municipiul Craiova este persoana juridica de drept public, cu capacitate juridica deplina, cu patrimoniu propriu, in care autonomia locala se realizeaza de catre autoritati ale administratiei publice locale, alese prin vot liber, egal, direct, secret si liber exprimat, consiliul local, ca autoritate deliberativa si primarul, ca autoritate executiva. Municipiul Craiova este subiect de drept fiscal, titular al Codului de inregistrare fiscala. Consiliul Local al Municipiului Craiova, ca organ deliberativ este format din 27 de consilieri, alesi prin vot universal, egal, direct, secret si liber exprimat, are initiativa si hotaraste in toate problemele de interes local, cu exceptia acelor date prin lege in competenta altor autoritati publice locale sau centrale. Potrivit prevederilor Legii nr. 351/2001, Sectiunea a IV-a-Reteaua de localitati, municipiul Craiova este localitate de rangul I municipiu de importanta nationala, cu influenta potentiala, la nivel european, resedinta judetului Dolj.

2.6 Factori interesați și rolul acestora, dacă este cazul

Nu este cazul

3 Descrierea produselor solicitate

3.1 Descrierea situației actuale la nivelul Autorității/entității contractante

La nivelul instituției este necesară achiziția unui router/firewall de mare viteză cu licență de securitate pentru 36 luni, împreună cu migrarea după vechiul firewall și configurarea serviciilor existente, împreună cu alte 3 routere fără licențe de securitate, de surse rackabile neîntreruptibile UPS

3000VA-2700W și a două data storage de rețea cu capacitate 6X6TB de 3,5 SATA în vederea susţinerii activităţilor de comunicații de date între sediile instituției și asigurării bunei funcționări a serviciului de comunicatii electronice la nivelul rețelei de IP a Primăriei Municipiului Craiova, dar si a realizării procedurii de backup date pentru datele critice.

3.2 Obiectivul general la care contribuie furnizarea produselor

Obiectivul general la care contribuie furnizarea produselor din cadrul contractului de furnizare tehnică de calcul: - Înlocuirea echipamentului actual, echipament de interconectare rețele de date, cu o solutie integrată router și firewall, antivirus și antimalware și de UPS-uri rackabile neîntreruptibile, întrucât acestea sunt uzate din punct de vedere fizic și moral iar pentru firewall-uri pe acestea licentele de securitate nu se mai pot prelungi.

3.3 Obiectivul specific la care contribuie furnizarea produselor

Obiectivul specific la care contribuie furnizarea produselor din cadrul contractului de furnizare tehnică de calcul, este dată de necesitatea schimbării echipamentelor actuale, deoarece:

a) Vechiile echipamente nu mai corespund cerinţelor actuale în domeniul telecomunicaţiilor, pe lângă uzura morală la aceste echipamente a apărut și uzura fizică, echipamentele generând erori pe porturi, porturi arse, datorită vechimii foarte mari, de peste 6 ani

b) Nu pot oferi acces în banda oferită de la ISP

c) Nu pot juca rol de firewall pentru că nu se mai pot adăuga pe ele licențe de securitate

d) Nu mai corespund cu politicile actuale de securitate

f) Nevoia de conectare prin mediu securizat la serverele folosite de Primăria Municipiului Craiova.

g) Securizarea accesului din locațiile secundare la nivel de municipiu pentru aplicațiile interne ale instituției.

3.4 Produsele solicitate și operațiunile cu titlu accesoriu necesar a fi realizate

- **Router/firewall de mare viteză cu licență de securitate pe 36 luni, migrare rețea și configurare - 1 buc**
- **Router/firewall de mare viteză fără licențe de securitate - 3 buc**
- **Sursa rackabilă neîntreruptibilă UPS 3000VA-2700W - 4 buc**
- **Storage retea cu capacitate de min 6 HDD fiecare în capacitate 6TB 3,5 SATA III - 2 buc.**

3.4.1 Produse solicitate

3.4.1.1 Router/firewall de mare viteza cu licență de securitate pe 36 luni, migrare rețea și configurare - 1 buc

Cerințe minime obligatorii:

- Integrare cu reteaua existenta a Primariei Municipiului Craiova, inclusiv cu celelalte routere existente, implementare protocoale de comunicare, configurare firewall, securizare retea interna, filtrare si curatarea traficului IP (atat dinspre internet cat si in reteaua locala) , teste, semnare PV de acceptanta ;
- Migrarea retelei interne (LAN) de pe routerul actual, in functionare, catre routerul nou, fara intreruperea serviciilor prin asigurarea continuitatii serviciilor si pastrarii configurarilor existente, sesiuni BGP, conexiuni de back-up, aplicatii ce trebuie integrate in noua arhitectura;
- Configurare acces securizat pentru aplicatii interne (VPN - MPLS) si integrarea LAN-ului in topologia retelei informatice la nivelul Primariei Municipiului Craiova;
- Asigurarea unei tranzitii eficiente a solutiei actuale catre noua solutie hardware/software in cadrul serviciului si integrarea lui cu echipamentele existente prin adaptarea politicilor de trafic securizat conform noilor provocari din IT si tinand cont de obligativitatea protectiei retelelor interne;
- Licenta de securitate inclusa pe 36 luni

Ofertantul va asigura :

- Furnizare + Instalare si migrarea echipament router/firewall de mare capacitate de trafic conform caracteristicilor descrise mai jos:

Caracteristici router / firewall cu licențe pentru 36 luni:

Denumire	**Echipament integrat de protecție a rețelei ce funcționează ca o soluție de securitate unificată**
Specificații hardware	• Interfețe GbE RJ-45: 12 • 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: 4 • Sloturi 10GE SFP+: 2 • Porturi consola RJ-45: 1 • Porturi USB: 1 • Dimensiune: 1U • Alimentare redundanta
Caracteristici	• Trafic firewall (1518/512/64 byte pachete UDP): 20/18/10 Gbps • Latenta Firewall: 4.97 µs • Trafic Firewall măsurat in pachete per secunda: 15 Mpps • Trafic IPSec VPN (512 byte packets): 11.5 Gbps • Trafic IPS: 2.6 Gbps • Trafic NGFW: 1.6 Gbps

	• Performanta SSL Inspection: 1 Gbps • Număr de tunele IPSec VPN site-to-site: 2.000 • Număr de clienți IPSec VPN: 16.000 • Trafic SSL-VPN: 1 Gbps • Număr de clienți concurenți SSL-VPN: 500 • Număr de sesiuni concurente TCP: 1.500.000 • Număr de sesiuni noi pe secundă TCP: 56.000 • Număr de politici de securitate: 10.000 • Număr de instanțe virtuale: 10 • Număr de AP-uri administrate (total/tunnel mode): 128/64 • Numar de switch-uri administrate: 32 • Trafic CAPWAP: 15 Gbps • Număr de token-uri OTP administrate: 5.000

Funcționalități generale	• Echipament integrat de securitate cu funcționalități simultane de:
	  • Firewall de tip stateful
	  • Router cu suport pentru protocoale de rutare dinamice
	  • Posibilitate de instalare in 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 si in 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 si platforma hardware apartin aceluiași producător
	• Conformitate cu: CE, CB

Funcționalități securitate	
Funcționalități firewall	• Funcționalități NAT, PAT si 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 si FTP • Suport pentru proxy chaining cu balansare de sesiuni prin proxy-uri multiple pentru funcționalitatea proxy explicit • Suport WINS • 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 si afișare al reputației utilizatorilor din rețea pe baza de scor dedus in mod configurabil din activitatea detectata prin mecanismele de inspecție de blocarea a atacurilor, blocare malware, filtrare web, firewall si inspecție a traficului de aplicații.
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 si L2TP VPN Client Pass Through • Funcționalitate "Hub and Spoke" IPSec VPN • Autentificare IKE prin certificate X.509 - suport pentru RSA si 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 in mod tunel si in 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 in cadrul sesiunii SSL VPN de restul aplicațiilor ce rulează pe stațiile utilizatorilor si 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 • Producătorul are in portofoliu client de VPN IPSec si SSL propriu, care are si funcționalități de: antivirus, filtrare web, filtrare a traficului de aplicații
Funcționalități Antivirus	• 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 si Flow-Based • Opțiune pentru detecția malware prin sandboxing de tip Cloud-Based al fișierelor suspecte, oferita de producător • Update-uri automate de semnături malware

	• Protecție împotriva rețelelor botnet si site-urilor de tip phishing pe baza de reputație a adreselor IP si a URL-urilor accesate de utilizatori
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 in funcție de URL/cuvânt cheie sau expresie in conținutul paginilor web • Blocare a conexiunilor in 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 activitatii web a utilizatorilor • Posibilitate de înștiințare a utilizatorilor, prin afișarea informațiilor in cadrul unui browser web, privind paginile web blocate
Funcționalități sistem de control al aplicațiilor	• Identificarea si controlul a peste 5000 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 si Risc • Monitorizare aplicațiilor cu rata cea mai mare de consum de banda • Monitorizarea aplicațiilor pe baza IP/Utilizator • Suport pentru decriptarea si inspectarea sesiunilor SSH • Suport pentru blocarea aplicațiilor utilizate in cadrul rețelelor de tip Botnet • Posibilitate de definire a semnăturilor de aplicație personalizate • Posibilitate de înștiințare a utilizatorilor, prin afișarea informațiilor in cadrul unui browser web, privind traficul de aplicații blocat
Funcționalități sistem de prevenire a intruziunilor/atacurilor (IPS)	• Protecție pentru peste 16.000 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 si IPv6 DoS/DDoS
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 si e-mail • Update-uri automate si in timp real
Funcționalitate Data Leak Prevention	• In caz de scurgere de informații trebuie sa permită blocarea si arhivarea conversației pe protocoale de email, HTTP, FTP si variantele criptate SSL; • Blocare după tip si dimensiune fișier

Funcționalități sistem de verificare a stațiilor (Endpoint Control)	• 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	
Funcționalități rețea si rutare	• 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 si 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 interfetelor in zone de securitate • Rutare intre zonele de securitate • Policy-based routing • Suport VRRP si 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 in IP • Suport NAT64, DNS64, NAT46, NAT66 • Suport LLDP

Funcționalitate Wireless Controller	• Modul wireless controller pentru thin-AP-uri integrat cu următoarele funcționalități:
	  • Detecție si suprimare a AP-urilor neînregistrate in controller;
	  • Selecție automata a canalului pentru AP in 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.
	  • 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 utilizarii spectrului de frecvente radio
Funcționalități Traffic Shaping	• Limitare/garantare/prioritizare a benzii de trafic prin politici • Traffic Shaping per aplicație si adresa IP • Suport pentru DSCP • Limitare a cotei de trafic (per adresa IP) • Suport pentru ToS
Funcționalități High Availability - HA	• Funcționare Active-Active, Active-Passive • Funcționalitate Stateful Failover (Firewall si VPN) • Detectare si notificare pentru echipament nefuncțional • Monitorizarea conexiunii la rețea • Funcționalitate Link Failover
Funcționalități de administrare, logare, autentificare a utilizatorilor	
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
Funcționalități de logare si monitorizare	
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 in rețea ce nu au instalat un client software de stație (client endpoint)
Condiții de alimentare	• Alimentare curent alternativ 100-240V, 50-60 Hz • Consum maxim de putere: 29.5 W
Condiții de mediu	• Temperatura de operare: 0 – 40 grade Celsius • Umiditate: 10–90 %, fara condens

Garanție si suport	• Solutia va beneficia de minimum trei ani de suport ce va include:
	  • Inlocuirea echipamentului in caz de defectiune hardware
	  • Suport tehnic din partea producatorului 7 zile pe saptamana, 24 de ore pe zi, in regim Next Business Day
	  • Update firmware versiuni minore si majore
	  • Soluția va beneficia de update-uri automate de semnături de securitate pentru îndeplinirea funcționalităților de Antivirus, Web Filtering,

	Antispam, Application Control si IPS timp de minimum trei ani

3.4.1.2 Router/firewall de mare viteză fără licențe de securitate și garantie 36 luni, migrare rețea și configurare - 3 buc

Cerințe minime obligatorii:

- Integrare cu rețeaua existentă a Primăriei Municipiului Craiova, inclusiv cu celelalte routere existente, implementare protocoale de comunicare, configurare firewall, securizare rețea internă, filtrare și curățarea traficului IP (atât dinspre internet cât și în rețeaua locală), teste, semnare PV de acceptantă ;
- Migrarea rețelei interne (LAN) de pe routerul actual, în funcționare, către routerul nou, fără întreruperea serviciilor prin asigurarea continuității serviciilor și păstrării configurărilor existente, sesiuni BGP, conexiuni de back-up, aplicații ce trebuie integrate în noua arhitectură;
- Configurare acces securizat pentru aplicații interne(VPN - MPLS) și integrarea LAN-ului în topologia rețelei informatice la nivelul Primăriei Municipiului Craiova;
- Asigurarea unei tranziții eficiente a soluției actuale către noua soluție hardware/software în cadrul serviciului și integrarea lui cu echipamentele existente prin adaptarea politicilor de trafic securizat conform noilor provocări din IT și tinând cont de obligativitatea protecției rețelelor interne;

Ofertantul va asigura :

- Furnizare + instalare și migrarea echipamentului router/firewall de mare capacitate de trafic conform caracteristicilor descrise mai jos:

Caracteristici router / firewall fără licente:

Denumire	**Echipament integrat de protecție a rețelei ce funcționează ca o soluție de securitate unificată**
Specificații hardware	• Interfețe GbE RJ-45: 4 • Interfete WAN/DMZ Gbe RJ-45: 1 • Porturi consola RJ-45: 1 • Porturi USB: 1 • Dimensiune: Desktop
Caracteristici	• Trafic firewall (1518/512/64 byte pachete UDP): 5/5/5 Gbps • Latenta Firewall: 2.97 µs • Trafic Firewall măsurat in pachete per secunda: 7.5 Mpps • Trafic IPSec VPN (512 byte packets): 4.4 Gbps • Trafic IPS: 1 Gbps • Trafic NGFW: 800 Mbps • Performanta SSL Inspection (IPS, HTTPS): 310 Mbps • Număr de tunele IPSec VPN site-to-site: 200 • Număr de clienți IPSec VPN: 250 • Trafic SSL-VPN: 490 Mbps

	• Număr de clienți concurenți SSL-VPN: 200 • Număr de sesiuni concurente TCP: 700.000 • Număr de sesiuni noi pe secundă TCP: 35.000 • Număr de politici de securitate: 5.000 • Număr de instanțe virtuale: 10 • Număr de AP-uri administrate (total/tunnel mode): 16/8 • Numar de switchuri administrate: 8 • Trafic CAPWAP: 3.5 Gbps • Număr de token-uri OTP administrate: 500

Funcționalități generale	• Echipament integrat de securitate cu funcționalități simultane de:
	  • Firewall de tip stateful
	  • Router cu suport pentru protocoale de rutare dinamice
	  • Posibilitate de instalare in 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 si in 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 si platforma hardware apartin aceluiași producător
	• Conformitate cu: CE, CB

Funcționalități securitate	
Funcționalități firewall	• Funcționalități NAT, PAT si 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 si FTP • Suport pentru proxy chaining cu balansare de sesiuni prin proxy-uri multiple pentru funcționalitatea proxy explicit • Suport WINS • 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 si afișare al reputației utilizatorilor din rețea pe baza de scor dedus in mod configurabil din activitatea detectata prin mecanismele de inspecție de blocarea a atacurilor, blocare malware, filtrare web, firewall si inspecție a traficului de aplicații.
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 si L2TP VPN Client Pass Through • Funcționalitate "Hub and Spoke" IPSec VPN • Autentificare IKE prin certificate X.509 - suport pentru RSA si 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 in mod tunel si in 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 in cadrul sesiunii SSL VPN de restul aplicațiilor ce rulează pe stațiile utilizatorilor si 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 • Producătorul are in portofoliu client de VPN IPSec si SSL propriu, care are si funcționalități de: antivirus, filtrare web, filtrare a traficului de aplicații
Funcționalități Antivirus	• 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 si Flow-Based • Opțiune pentru detecția malware prin sandboxing de tip Cloud-Based al fișierelor suspecte, oferita de producător • Update-uri automate de semnături malware • Protecție împotriva rețelelor botnet si site-urilor de tip phishing pe baza de reputație a adreselor IP si a URL-urilor accesate de utilizatori

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 in funcție de URL/cuvânt cheie sau expresie in conținutul paginilor web • Blocare a conexiunilor in 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 activitatii web a utilizatorilor • Posibilitate de înștiințare a utilizatorilor, prin afișarea informațiilor in cadrul unui browser web, privind paginile web blocate
Funcționalități sistem de control al aplicațiilor	• Identificarea si controlul a peste 5000 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 si Risc • Monitorizare aplicațiilor cu rata cea mai mare de consum de banda • Monitorizarea aplicațiilor pe baza IP/Utilizator • Suport pentru decriptarea si inspectarea sesiunilor SSH • Suport pentru blocarea aplicațiilor utilizate in cadrul rețelelor de tip Botnet • Posibilitate de definire a semnăturilor de aplicație personalizate • Posibilitate de înștiințare a utilizatorilor, prin afișarea informațiilor in cadrul unui browser web, privind traficul de aplicații blocat
Funcționalități sistem de prevenire a intruziunilor/atacurilor (IPS)	• Protecție pentru peste 16.000 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 si IPv6 DoS/DDoS
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 si e-mail • Update-uri automate si in timp real
Funcționalitate Data Leak Prevention	• In caz de scurgere de informații trebuie sa permită blocarea si arhivarea conversației pe protocoale de email, HTTP, FTP si variantele criptate SSL; • Blocare după tip si dimensiune fișier
Funcționalități sistem de verificare a stațiilor	• Integrare cu o aplicație software pentru securitate ce rulează pe stații

(Endpoint Control)	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	
Funcționalități rețea si rutare	• 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 si 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 interfetelor in zone de securitate • Rutare intre zonele de securitate • Policy-based routing • Suport VRRP si 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 in IP • Suport NAT64, DNS64, NAT46, NAT66 • Suport LLDP
Funcționalitate Wireless Controller	• Modul wireless controller pentru thin-AP-uri integrat cu următoarele funcționalități: • Detecție si suprimare a AP-urilor neînregistrate in controller; • Selecție automata a canalului pentru AP in 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. • 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 utilizarii spectrului de frecvente radio
Funcționalități Traffic Shaping	• Limitare/garantare/prioritizare a benzii de trafic prin politici • Traffic Shaping per aplicație si adresa IP • Suport pentru DSCP • Limitare a cotei de trafic (per adresa IP) • Suport pentru ToS
Funcționalități High Availability - HA	• Funcționare Active-Active, Active-Passive • Funcționalitate Stateful Failover (Firewall si VPN) • Detectare si notificare pentru echipament nefuncțional • Monitorizarea conexiunii la rețea • Funcționalitate Link Failover
Funcționalități de administrare, logare, autentificare a utilizatorilor	
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
Funcționalități de logare si monitorizare	
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 in rețea ce nu au instalat un client software de stație (client endpoint)
Condiții de alimentare	• Alimentare curent alternativ 100-240V, 50-60 Hz • Consum maxim de putere: 9.46 W
Condiții de mediu	• Temperatura de operare: 0 – 40 grade Celsius • Umiditate: 10–90 %, fara condens • Nivel zgomot: 0 dBA (fara ventilatoare)
Garanție si suport	• Solutia va beneficia de minimum trei ani de suport ce va include: • Inlocuirea echipamentului in caz de defectiune hardware • Suport tehnic din partea producatorului 7 zile pe saptamana, 24 de ore pe zi, in regim Next Business Day • Update firmware versiuni minore si majore • Garantie 3 ani

3.4.1.3 Sursa rackabila neîntreruptibilă UPS 3000VA-2700W - 4 buc

Specificatii tehnice:

- Rack/Tower Convertible Design
- Patented LCD Display can be rotated
- True Online Double Conversion
- Output power factor 0.9
- Hot-Swappable Battery
- Efficiency up to 90%
- Estimated Remaining Time displayed on the LCD
- Support economic (ECO) operation mode
- Support generator input
- Matching Battery Pack
- Self-testing at UPS startup
- Cold Start
- USB + RS232 management interfaces Options: SNMP/Relay card Emergency power off function (EPO) Drivere, Firmware Si Alte Documente

3.4.1.4 Storage retea cu capacitate de min 6 HDD fiecare în capacitate 6TB 3,5 SATA III - 2 buc.

Specificații tehnice:

Hardware Specifications		
Procesor	CPU Model	AMD Ryzen
	CPU Quantity	1
	CPU Core	4
	CPU Architecture	64-bit
	CPU Frequency	2.2 GHz
Memorie	Memorial sistemului	4 GB DDR4 ECC SODIMM
	Modul memories preinstlat	4 GB (4 GB x 1)
	Numeral de sloturi de memorie	2
	Capacitate maxima memorie	32 GB (16 GB x 2)
Storage	Numar de bay-uri (locuri pentru HDD) Capacitate minim instalata	8 36 TB pe 6 HDD
	Tipuri de hard-disk-uri compatibile	• 3.5" SATA HDD • 2.5" SATA HDD • 2.5" SATA SSD
Porturi externe	RJ-45 1GbE LAN Port	4
	USB 3.2 Gen 1 Port*	2
	Expansion Port	1
	Expansion Port Type	eSATA
PCIe	PCIe Expansion	1 x Gen3 x8 slot (x4 link)
Grad ocupare in cabinet metalic	Form Factor (RU)	2U
	Posibilitatea de a fi instalat in cabinet metalic	

	Posibilitatea de a fi instalat in cabinet metalic	
	System Fan	80 mm x 80 mm x 2 pcs
	Fan Speed Mode	• Full-Speed Mode • Cool Mode • Quiet Mode
	Zgomot	53.5 dB(A)
	Programare Power On / Off	
	Wake on LAN / WAN	
	Sursa alimentare	350 watts
	Sursa alimentare redundanta	
	AC Input	100 V to 240 V AC, 50/60 Hz,
	Puterea consumată	61.94 watts (Access) 29.98 atts (HDD Hibernation)

3.4.2 Disponibilitate, dacă este cazul

Nu este cazul.

3.5 Extensibilitate/Modernizare, dacă este cazul

Nu este cazul.

3.5.1 Garanție

Perioada de garanție acordată produselor va fi de 36 luni pentru routere si firewall, dar si pentru storage-ul de retea, respectiv 24 luni pentru surse rackabile neîntreruptibile, in condițiile certificatului de garanție calculate de la data recepției prin semnarea fără obiecții a procesului verbal de recepție încheiat între furnizor și achizitor.

In perioada de garanție reparațiile pentru posibilele defecțiuni acoperite de garanție vor fi suportate de către furnizor. Piesele de schimb care fac obiectul garanției pentru produs vor fi asigurate pentru o perioada cel puțin egala cu garanția comerciala. La orice reparație executata se vor folosi numai piese noi de origine certificate/ omologate si agreate de producătorul produselor conform reglementarilor si normelor tehnice in vigoare.

În cazul componentelor software, serviciile de garantie includ constatarea defectelor și remedierea lor în termenele stabilite în procedura de garantie. Remedierea defectelor se va realiza cu respectarea termenelor privind severitatea lor.

3.5.2 Livrare, ambalare, etichetare, transport și asigurare pe durata transportului

Termenul de livrare este cel mult 21 de zile lucrătoare de la data comenzii. Un produs este considerat livrat când toate activitățile în cadrul contractului au fost realizate și produsul/echipamentul este acceptat de Autoritatea/entitatea contractantă.

Produsele vor fi livrate cantitativ la locul indicat de Autoritatea/entitatea contractantă pentru

fiecare produs în parte. Fiecare produs va fi însoțit de toate subansamblele/părțile componente necesare punerii și menținerii în funcțiune.

Contractantul va ambala și eticheta produsele furnizate astfel încât să prevină orice daună sau deteriorare în timpul transportului acestora către destinația stabilită, respectiv Centru Multifuncțional Str. Târgului, nr .26, magazia unității din cadrul Primăriei Municipiului Craiova.

Pentru toate echipamentele livrate, ofertantul va prezenta o fişă de produs din partea producătorului, care să conţină minim următoarele informaţii: denumirea producătorului, date şi specificaţii tehnice despre produs, precum şi datele de contact ale producătorului.

Echipamentele vor avea toate componentele necesare conexiunilor (cabluri). Acestea vor intra în valoarea ofertei.

Dacă este cazul, ambalajul trebuie prevăzut astfel încât să reziste, fără limitare, manipulării accidentale, expunerii la temperaturi extreme, sării şi precipitaţiilor din timpul transportului şi depozitării în locuri deschise. În stabilirea mărimii şi greutăţii ambalajului Contractantul va lua în considerare, acolo unde este cazul, distanta față de destinația finală a produselor furnizate și eventuala absență a facilităților de manipulare la punctele de tranzitare.

Transportul şi toate costurile asociate sunt în sarcina exclusivă a contractantului. Produsele vor fi asigurate împotriva pierderii sau deteriorării intervenite pe parcursul transportului şi cauzate de orice factor extern.

Contractantul este responsabil pentru livrarea în termenul agreat al produselor şi se consideră că a luat în considerare toate dificultăţile pe care le-ar putea întâmpina în acest sens şi nu va invoca nici un motiv de întârziere sau costuri suplimentare.

3.5.3 Operaţiuni cu titlu accesoriu, dacă este cazul

Nu este cazul.

3.5.4 Mediul in care este operat produsul

Nu este cazul.

3.5.5 Constrângeri privind locaţia unde se va efectua livrarea

Transportul se va efectua de catre si pe cheltuiala furnizorului pâna la sediul beneficiarului, respectiv Primaria Municipiului Craiova - Centru Multifuncțional Str. Târgului, nr. 26, magazia instituției.

Livrarea şi recepţia produselor se va efectua în timpul programului de lucru: de luni până joi între orele 08.00-16.30 şi vineri între orele 08.00-14.00, modul de comunicare dintre furnizor si autoritate facandu-se pe e-mail sau fax

3.6 Atribuțiile și responsabilitățile Părților

Obligaţii achizitor

- 1. Asigurarea suportului tehnic (documentaţie, acces la instalaţie) la solicitarea furnizorului şi asumarea responsabilității pe calitatea datelor puse la dispoziție
- 2. Asigurarea fondurilor pentru plăţile în termen datorate furnizorului
- 3. Să achiziţioneze, respectiv să cumpere şi să plătească preţul convenit în contract
- 4. Să recepţioneze produsele în termenul convenit
- 5. Să facă plata după recepţie, în termen de maxim 30 de zile, pe baza facturii emise, depusă la sediul autoritatii contractante, cu ordin de plata prin Trezorerie
- 6. Exploatarea produsului conform instrucțiunilor puse la dispoziție de furnizor / producător

Obligaţii ofertant/furnizor

Furnizorul echipamentelor este responsabil pentru furnizarea produselor în condițiile prezentului caiet de sarcini.

Furnizorul se obligă să asigure, pentru echipamentele furnizate o perioada de garanție de minim 36 luni pentru router, respectiv 24 luni pentru surse rackabile neîntreruptibile. Pe toata perioada de garanţie, furnizorul are obligatia de a asigura cu titlu gratuit asistență la cerere și remedierea/repararea oricăror defectiuni care nu sunt generate din culpa achizitorului, inclusiv înlocuirea utilajului defect cu unul nou dacă repararea nu este posibilă.

Responsabilitatea integrităţii pe timpul transportului, manipulării până la destinația finală a produselor este în sarcina furnizorului.

4 Documentații ce trebuie furnizate Autorității/entității contractante în legătură cu produsul

Contractantul va furniza Autorității/entității contractante declarația de conformitate, garanția și factura pentru produsele livrate.

5 Recepția produselor

Recepția produselor se va efectua pe baza de proces verbal semnat de Contractant și Autoritatea/entitatea contractantă în termen de maxim 7 zile de la livrarea produselor în cantitatea solicitată la locația indicată de instituție. Dacă în cadrul recepției se constată că nu au fost îndeplinite în totalitate condițiile de trecere a recepției, furnizorul este obligat să remedieze neconformitățile identificate în decurs de 5 zile de la constatarea lor.

6 Modalități si condiții de plata

Sursa/sursele de finanțare prin care se vor asigura fondurile necesare pentru realizarea achiziției: bugetul local.

Contractantul va emite factura pentru produsele livrate pe care o va încărca în sistemul național privind factura RO e-Factura conf. OUG nr. 120/2021, cu modificările și completările ulterioare.

Factura va avea menționat numărul contractului, datele de emitere și de scadența ale facturii respective.

Factura va fi emisă după semnarea de către Autoritatea/entitatea contractantă a procesului verbal de recepție cantitativă. Procesul verbal de recepție cantitativă va însoți factura și reprezintă elementul necesar realizării plății, împreună cu celelalte documente justificative prevăzute mai jos:

- certificatul de calitate și garanție;
- avizul de expediție a produsului;

7 Cadrul legal care guvernează relația dintre Autoritatea/entitatea contractantă și Contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă)

Pe perioada derulării Contractului, Contractantul este responsabil pentru realizarea activităților în conformitate cu cerintele caietului de sarcini și implementarea celor mai bune practici, în conformitate cu regulile și regulamentele existente la nivel național și la nivelul Uniunii Europene.

In realizarea activităților sale în cadrul Contractului Contractantul trebuie să aibă în vedere:

i. informațiile aplicabile realizării lucrărilor în general (astfel cum sunt descrise în acest Caiet de sarcini, precum și în legislația aplicabilă;

ii. regulile aplicabile în mod specific realizării de servicii a căror execuție face obiectul Contractului ce va rezulta din prezenta procedură de atribuire.

Prin depunerea unei Oferte ca răspuns la cerințele din prezentul Caiet de sarcini, se prezumă că Contractantul, are cunoștințe și are în vedere toate și orice reglementări aplicabile și că le-a luat în considerare la momentul depunerii Ofertei sale pentru atribuirea Contractului.

În cazul în care, pe parcursul derulării Contractului, apar schimbări legislative de natură să influențeze activitatea Contractantului în raport cu cerințele stabilite prin prezentul Caiet de sarcini, Contractantul are obligația de a informa Autoritatea contractanta cu privire la consecințele asupra activităților sale ce fac obiectul Contractului și de a își adapta activitatea, de la data și în condițiile în care sunt aplicabile.

În cazul în care vreuna din regulile generale sau specifice nu mai sunt în vigoare sau au fost modificate conform legii la data depunerii Ofertei, se consideră că regula respectivă este automat înlocuită de noile prevederi în vigoare conform legii și că Ofertantul/Contractantul are cunoștință de aceste schimbări și le-a avut în vedere la depunerea Ofertei sale în baza acestui Caiet de sarcini.

Contractantul va fi ținut deplin responsabil pentru subcontractanții acestuia, chiar și în situația în care au fost în prealabil agreați cu Autoritatea Contractantă, urmând să răspundă față de

Autoritatea Contractantă pentru orice nerespectare sau omisiune a respectării oricăror prevederi legale și normative aplicabile.

Autoritatea Contractantă nu va fi ținută responsabilă pentru nerespectarea sau omisiunea respectării de către Contractant sau de către subcontractanții acestuia a oricărei prevederi legale sau normative aplicabile.

În executarea Contractului, Ofertantul devenit Contractant are obligația de a respecta obligațiile aplicabile în domeniul mediului, social și al muncii instituite prin dreptul Uniunii, prin dreptul național, prin acorduri colective sau prin dispozițiile internaționale de drept în domeniul mediului, social și al muncii enumerate în anexa X la Directiva 2014/24, respectiv:

a. Convenția nr. 87 a OIM privind libertatea de asociere și protecția dreptului de organizare;

b. Convenția nr. 98 a OIM privind dreptul de organizare și negociere colectivă;

c. Convenția nr. 29 a OIM privind munca forțată;

d. Convenția nr. 105 a OIM privind abolirea muncii forțate;

e. Convenția nr. 138 a OIM privind vârsta minimă de încadrare în muncă;

f. Convenția nr. 111 a OIM privind discriminarea (ocuparea forței de muncă și profesie);

g. Convenția nr. 100 a OIM privind egalitatea remunerației;

h. Convenția nr. 182 a OIM privind cele mai grave forme ale muncii copiilor;

i. Convenția de la Viena privind protecția stratului de ozon și Protocolul său de la Montreal privind substanțele care epuizează stratul de ozon;

j. Convenția de la Basel privind controlul circulației transfrontaliere a deșeurilor periculoase și al eliminării acestora (Convenția de la Basel);

k. Convenția de la Stockholm privind poluanții organici persistenți (Convenția de la Stockholm privind POP);

Informațiile detaliate privind reglementările care sunt în vigoare și se referă la condițiile de muncă și protecția muncii, securității și sanătșii in munca, protectiei sociale si persoanelor varstnice, se pot obtine de pe site-ul: http://www.mmuncii.ro.

Informatiile detaliate privind reglementarile care sunt in vigoare si se refera la conditiile de mediu si protectia mediului, se pot obtine de pe site-ul: http://www.mmediu.ro.

Actele normative și standardele indicate mai jos sunt considerate indicative și nelimitative; enumerarea actelor normative din acest capitol este oferită ca referință și nu trebuie considerată limitativă.

8 Managementul/Gestionarea Contractului și activități de raportare în cadrul Contractului, dacă este cazul

Autoritatea Contractantă este responsabilă pentru derularea procedurii de atribuire a Contractului, monitorizarea execuției Contractului și efectuarea plăților către Contractant, conform Contractului.

Autoritatea Contractantă și Contractantul își transmit reciproc notificări de îndată ce una dintre părți devine conștientă de apariția în perioada imediat următoare a unui eveniment sau a unei situații care ar putea:

- Să conducă la întârzierea termenelor de predare, generând nerespectarea termenului de finalizare a serviciilor din Contract.
- Să afecteze activitatea Autorității Contractante sau a altor factori interesați identificați în legătura cu serviciile incluse în scopul Caietului de Sarcini.

Îmi asum responsabilitatea privind realitatea și legalitatea în solidar cu întocmitorul înscrisului *Director Executiv, Claudiu Popescu* *Data:* 16.07.2024 *Semnătura:* *Șef Serviciu, Claudia Lăpădat* *Data:* 16.07.2024 *Semnătura:*	*Îmi asum responsabilitatea pentru fundamentarea, realitatea și legalitatea întocmirii acestui act oficial* *Expert, Mariana Ioana* *Data:* 16.07.2024 *Semnătura:*