Nr.6429/AP/31.10.2022

SOLICITARE DE OFERTĂ

În vederea achiziţionării prin **cumpărare directă**, vă solicităm să ne transmiteţi până la data de **02.11.2022, inclusiv, oferta de preţ** în lei fără TVA, la adresa de e-mail stefania.plescan@uaic.ro pentru următoarele produse:

Nr. lot	**Denumire produs** *Specificaţii tehnice minime*	Cant.
1	**Software antivirus Bitdefender Small Office Security pentru 5 dispozitive, valabilitate licenta: 2 ani** *sau echivalent* - Cheia de licență se va livra în format electronic la o adresa de e-mail ce va fi comunicata impreuna cu comanda - Termen de livrare: 5 zile lucratoare	1
2	**Pachet extensie 60 de computere la cheia de licentiere KQ4226B Bitdefender Gravity Zone Business Security** sau echivalent. Principalele caracteristici tehnice care trebuie să se regăsească ca funcționale și incluse în produsul ofertat sunt: - Produsul trebuie să ofere posibilitatea de administrare centralizată prin intermediul unei console de administrare în cloud prin interfata web, platforma cloud trebuie să fie administrata fizic și virtual de personal aflat sub incidenta Regulamentului General privind Protecția Datelor (RGPD) 679/2016; - Prin intermediul licenței, beneficiarul va avea acces la suport tehnic minim în intervalul 7.30-20.00, în fiecare zi lucrătoare, în limba română; - Produsul trebuie să fie licențiat către Autoritatea contractanta pe o perioadă de minim 2 ani. Licența va permite instalarea pe stații de lucru din birourile și laboratoarele Facultății de Psihologie și Științe ale Educației din cadrul Universității "Alexandru Ioan Cuza" din Iași; - Produsul trebuie să includă actualizarea versiunii, respectiv a generației de program; - Produsul trebuie sa includă actualizarea bazei de date cu semnături și a motoarelor de scanare; - Produsul trebuie să permită identificarea potențialelor atacuri printr-o singură interfață web pentru toate calculatoarele Facultății de Psihologie și Științe ale Educației din UAIC. - Produsul trebuie să permită definirea de către administrator a unor liste de tip whitelist cu sit-uri care sunt excluse de la filtrarea URL; - Produsul trebuie să permită definirea de către administrator a unor liste de tip blacklist pentru filtrarea URL în vederea prevenirii traficului cu activități dăunatoare; - Produsul va asigura cel puțin următoarele componente de securitate: tehnologii anti-malware (antivirus și antispyware incluse) care să includă tehnici de învățare automată (ML) care să includă minim 40 mii de unelte statice și dinamice antrenate permanent pe exemple de fișiere curate sau malițioase culese dintr-un bazin de minim 500 milioane de end-pointuri la nivel global, tehnologii care blochează procesele de phishing respectiv altele cu comportamente frauduloase, controlul clienților să se realizeze pe bază de consolă de management centralizată cu interfața user-friendly, care oferă posibilitatea de configurare și management în timp real a politicilor configurabile de către utilizatorul autorizat de Autoritatea contractantă și care să includă mecanisme de firewall, scanare a device-urilor conectate prin USB, și controlul conținuturilor web, cu posibilitate de creare de categorii de URL-uri pentru controlul conținuturilor web, configurarea și managementul pachetelor pentru stațiile de tip client, forțarea stațiilor de tip client să efectueze actualizările de pachet pentru client și a politicilor de securitate folosite pe acesta în timp real pentru toți cei 60 de clienți simultan, produsul să asigure securitatea stațiilor de tip client și în situația în care numărul de licențe necesare crește neașteptat și depășește numărul de licențe achiziționate, să permită	1

	instalarea în continuare a pachetelor client dar să avertizeze utilizatorul autorizat de acest eveniment prin interfaţa web de administrare, produsul să asigure accesul utilizatorului autorizat la consola de management prin interfaţă web şi în situaţii precum expirarea termenului de licenţiere sau depăşirea numărului de dispozitive protejate de pachetele client instalate; - Interfaţa de configurare a pachetelor client trebuie să permită configurarea acestora pentru utilizarea adecvată a următoarelor tehnologii de securitate: pachetele client trebuie să includă tehnologii pentru detectie si blocare impotriva mecanismelor de exploatare a memoriei si respectiv a aplicatiilor vulnerabile la apelarea API-urilor, la stive pilot, la programe orientate pe raspuns etc.; pachetele client trebuie să includă tehnologii de filtrarea traficului pe reţea cu cablu sau fără care să scaneze traficul care intră în staţia de tip client, inclusiv SSL, HTTP si HTTPS, astfel încât să împiedice download-area de software dăunător către staţia de tip client; pachetele client trebuie să includă inspector de procese care să opereze în regim "0 încredere" şi care să monitorizeze continuu procesele care rulează în sistemul de operare; pachetele client configurate prin interfaţa aceasta de configurare trebuie să aibă incluse în mod implicit funcţionalităţile de mai jos: - Pachetele client trebuie să includă componente care să identifice modele de atacuri de tip ransomware în fazele de preexecuţie şi cel tîrziu execuţie bazându-se pe exemple culese dintr-un bazin de peste 500 milioane de endpointuri la nivel global; - Pachetele client trebuie să includă componente care să neutralizeze automat ameninţările prin terminarea proceselor, carantinare sau ştergerea de fişiere dăunătoare şi refacerea la versiunea dinainte de schimbările maliţioase. - Pachetele client vor rula pe staţii de lucru si servere fizice (desktopuri, laptopuri, dispozitive mobile), fiecare având unul din următoarele sisteme de operare: Microsoft Windows 7,8,8.1,10,11 x86/x64, macOS Catalina, Monterey, Sierra, distribuţii Linux Ubuntu, CENToS, trebuie deci să fie compatibile si configurabile pentru acestea; - Pachetele client trebuie să includă componente care pornesc împreună cu sistemul de operare, rămân în permanenţă în memorie şi scanează toate fişierele care sunt deschise, salvate sau rulate pe computer, laptop, server; - Pachetele client trebuie să neutralizeze pericolele detectate prin metode precum terminarea proceselor, carantinare, ştergerea fişierelor sau derulare la versiuni anterioare a modificărilor dăunătoare; - Pachetele client trebuie să ofere cel puţin tehnologii de scanare locală; - Pachetele client trebuie să includă tehnologii care să optimizeze viteza de scanare a fişierelor; - Pachetele client trebuie să scaneze inclusiv traficul de tip email şi filtrarea ataşamentelor e-mailurilor suspecte a fi malware; - Pachetele client trebuie să includă componente de protecţie a datelor trimise şi primite prin protocoalele HTTP, HTTPS si FTP;	

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

	- Pachetele client trebuie să includă componente care monitorizează activitatea unui program în sistem şi dacă acesta este considerat periculos, activitatea sa să fie blocată; - Pachetele client trebuie să includă protecţie împotriva programelor care exploatează vulnerabilităţile, inclusiv a celor care folosesc aşa numitele vulnerabilităţi zero-day, dar şi ameninţările care nu au fost înregistrate în baza de date cu semnături; - Pachetele client trebuie să includă scanarea pe bază de semnături cât şi analiza euristică; - Pachetele client trebuie să includă tehnologii care să prevină infecţiile cu programe periculoase prin intermediul dispozitivelor externe ataşate staţiilor de lucru (memorii USB, dispozitive Bluetooth, CD/DVD playere, dispozitive de stocare, etc.); - Pachetele client trebuie să permită utilizatorului autorizat de Autoritatea contractantă să transmită staţiilor de tip client, în timp real, politicile pentru filtrarea traficului şi comenzilor de actualizare a produsului; - Pachetele client trebuie să includă tehnologii pentru detectarea automată a vulnerabilităţilor din sistemul de operare. - Pachetele client trebuie să ofere rapoarte detaliate către consola de administrare accesibilă prin interfaţă web; - Pachetele client trebuie să includă tehnologii pentru scanarea traficului de intrare în staţiile client pentru activităţi tipice atacurilor de reţea şi să blocheze activitatea din reţea care provine de la computerul care iniţiază atacul; - Produsul trebuie să includă un mecanism de auto-protecţie prin parolă administrată centralizat din interfaţa web, care să prevină distrugerea sau ştergerea fişierelor aplicaţiei din sistem, proceselor din memorie şi intrările în sistemul de regiştri; - La cerere, se va acorda suport tehnic la instalarea produsului prin intermediul suportului tehnic menţionat anterior, în intervalul de timp menţionat anterior. - Cheia de licenţă se va livra în format electronic la o adresa de e-mail ce va fi comunicata impreuna cu comanda - Termen de livrare: 5 zile lucratoare	
3	**Licenta Bitdefender Antivirus Plus cheie unica pentru 300 dispozitive, valabilitate 3 ani – innoire pachet** *sau echivalent* Antivirus plus 300 licente 3 ani innoire cheiei unica • **Protectie completa si in timp real a datelor** - impotriva tuturor tipurilor de amenintari electronice, de la virusi, viermi si troieni la ransomware, exploit-uri de tip ziua zero, rootkit-uri si programe spion. • **Evaluarea vulnerabilitatilor** - verifica PC-urile pentru a identifica orice software neactualizat si vulnerabil, actualizari de securitate Windows care lipsesc si setari de sistem potential nesigure, indicand cea mai buna metoda de remediere. • **Anti-tracker** - blocheaza tracker-ele care colecteaza date si permite vizualizarea si gestionarea informatiilor pentru fiecare site accesat. • **Advanced Threat Defense** - descopera si blocheaza amenintarile avansate si pe cele de tip ransomware. • **Straturi multiple de protectie anti-ransomware** - protejeaza datele personale (documente, poze, videoclipuri, muzica) impotriva unor eventuale atacuri ransomware.	

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

	• **Prevenire amenintari retea** - previne exploatarea vulnerabilitatilor sistemului si identifica activitatile suspecte la nivel de retea. • **Prevenirea atacurilor web** - blocheaza toate link-urile infectate si avertizeaza daca rezultatele de cautare pe internet sunt sigure pentru a fi accesate. • **Mediu de recuperare** - reporneşte calculatorul in modul Mediu de recuperare pentru curatare si recuperare • **Evaluare securitate retele Wi-Fi** • **Tranzactii bancare online sigure** • **Protectie in cadrul retelelor sociale** • **Antiphishing & Antifrauda** • **Stergere definitiva fisiere** • **Protectie fisiere** **CERINTE DE SISTEM** • **Sistem de operare: Microsoft Windows 7 cu Service Pack 1, Windows 8, Windows 8.1, Windows 10** • **Memorie (RAM): 2 GB** • **Spatiu liber disponibil pe hard disk: 2.5 GB** **innoire cheiei unica** - Cheia de licenţă se va livra în format electronic la o adresa de e-mail ce va fi comunicata impreuna cu comanda - Termen de livrare: 5 zile lucratoare	1

Specificaţiile tehnice care indică o anumită origine, sursă, producţie, un procedeu special, o marcă de fabrică sau de comerţ, un brevet de invenţie, o licenţă de fabricaţie, sunt mentionate doar pentru identificarea cu uşurinţă a tipului de produs şi NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificaţii vor fi considerate ca având menţiunea de « sau echivalent ».

Toate componentele si produsele vor fi noi si nefolosite(chei de licenţă, seriale etc.).

Criteriul de atribuire: preţul cel mai scăzut, in conditiile respectarii cerintelor solicitate. Atribuirea se va realiza pe fiecare lot in parte.

Se va specifica perioada de valabilitate a ofertei (minim 30 de zile) şi termenul de livrare al produselor.

La livrare produsele vor fi însoţite de declaraţii de conformitate/calitate şi factură fiscală.

Conform Legii 139/2022, contractantul are obligaţia de a emite facturi electronice şi de a le transmite Autorităţii Contractante prin sistemul RO e-factura.

Termenul de plată este:

a) 30 de zile calendaristice de la data la care factura electronica este disponibila spre descarcare de către Autoritatea Contractanta, din sistemul RO e-factura, daca receptia este anterioara acestei date;

a) 30 de zile calendaristice de la data receptiei daca factura electronica este disponibila spre descarcare de către Autoritatea Contractanta din sistemul RO e-factura, la data receptiei ori anterior acestei date.

Prin depunerea ofertei, ofertantul îşi exprimă implicit acceptul său asupra condiţiilor de valabilitate a ofertei, asupra termenului de plată, precum şi a termenului şi condiţiilor de livrare.

ŞEF SERVICIU ACHIZIŢII PUBLICE,
Ing. Gabriela ALEXOAIE

MINISTERUL EDUCAŢIEI UNIVERSITATEA „ALEXANDRU IOAN CUZA" DIN IAŞI SERVICIUL ACHIZIŢII PUBLICE ROMÂNIA

Intocmit,
Ec. Stefania Plescan

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126