УНИВЕРЗИТЕТ У НОВОМ САДУ

Пољопривредни факултет у Новом Саду

Трг Доситеја Обрадовића 8

Број:

Датум: 08.06.2020.

Захтев за покретање поступка јавне набавке

Шеф ИТ службе пољопривредног факултета из Новог Сада предлаже да се покрене поступак јавне набавке чији су предмет антивирус софтвер

(Обавезно приложити техничку спецификацију)

Шифра из општег речника набавки:

Позиција у плану набавки: 1.1.16

Процењена вредност набавке износи 400.000,00 без ПДВ-а, до које се дошло на следећи начин:

Процена је направљена на основу разговора са добављачима.

Тражено добро/радове/услуге на тржишту нуде следећи понуђачи:

1. LOGON DOO, Ruđera Boškovića 46, 21000 Novi Sad, info@logon.rs

2. EXTREME DOO, Starine Novaka 23/11, 11120 Beograd, softver@extreme.rs

3. IQ DOO, Danila Kiša 15, 21000 Novi Sad, office@iqcomputers.com

(Обавезно навести пун назив понуђача као и e-mail адресу)

Средства за набавку обезбеђена су: Сопствена средства

(Обавезно навести изворе финсирања набавке, ако су то поред сопствених прихода и буџетска срества, обавезно навести и по ком су основу добијена (број уговора, број и назив пројекта итд.))

За председника и чланове комисије предлажу се:

Милан Ковачевић

Дејан Поповић

Марко Вулић

Са набавком сагласан Са набавком сагласан

**Продекан за развој и**

**Шеф ИТ службе** **сарадњу с привредом** **Декан**

Милан Ковачевић Проф. др Драган Гламочић Проф. др Недељко Тица

**Техничке карактеристике софтвера**

1. **Опис и количина**

|  |  |  |
| --- | --- | --- |
| **Proizvod** | **Količina** | **Dužina zakupa licence** |
| Antivirus Endpoint Protection Advanced | 250 komada | 1 godina |

1. **Технички захтеви за коришћење и одржавање антивирусне заштите**

Softverski paket mora da uključi sledeće module:

• **Anti-Virus** - zaštitu od virusa, crva (worms), trojanaca, root-kitova, špijunskog softvera (spyware), adware-a, potencijalno neželjenog (PUA) i ostalog malicioznog softvera;

• **Malicious Traffic Detector** - mogućnost identifikacije i zaustavljanja komunikacije zaraženih radnih stanica sa kompromitovanim ili C&C serverima;

• **Behavior Monitoring** – Host Intrusion Prevention System (HIPS), zaštitu od nepoz- natih i “zero-day” pretnji;

• **LiveProtection** – automatska provera sumnjivih fajlova na nepoznate pretnje

• **Web Protection** – napredna zaštita od web pretnji sprečavanjem pristupa lokacijama koje su poznate kao maliciozne tj. sadrže maliciozni kod. Provera sajta se vrši u realnom vremenu. Zaštita takođe skenira preuzete podatke i proverava njihovu reputaciju;

• **Application Control** – mogućnost kontrolisanja izvršavanja aplikacija koje nisu mali- ciozne, ali koje je potrebno zabraniti za krajnjeg korisnika;

• **Device Control** – kontrola upotreba i načina upotrebe (read-only, full access) prenosivih memorija i mrežnih interfejsa (modem, Bluetooth, IrDA, USB, Wi-Fi);

• **Data control** – sistem sprečavanja i praćenja slanja određenih podataka sa računara. Pruža mogućnost da se ograniči slanje ili snimanje npr .xls fajla (ili bilo koje druge ek- stenzije). Postoji mogućnost provere sadržine dokumenta kako bi se sprečilo slanje po- dataka kao što su brojevi kreditnih kartica, JMBG ili drugi struktirani podaci koji su bit- ni za korisnike. Modul može da radi u silent (“alert only” za administratora) modu ili da izbacuje jasnu poruku ili upozorenje krajnjem korisniku o zabrani ili ograničenju;

• **Client Firewall** – klijentski firewall, sa Network Awareness funkcionalnosti. Omogućava konfigurianje polisa po tipu saobraćaja (dolazni/odlazni), protokolu i portu. Poseduje statefull inspection funkcionalnst;

• **PureMessage for Exchange** – antivirusna, antispam i content zaštita koja se integriše sa Exchange serverom. Softver takođe pruža mogućnost kontrole velićine e-mail poruke, maksimalan broj primaoca, neprimeren rečnik, itd;

• **Web control** – kontrola pristupa web sajtovima u odnosu na kategorizaciju. Modul takođe pruža mogućnost generisanja izveštaja po korisniku i tipu web sajta koji je posećivan. Zaštita funkcioniše unutar i van mreže preduzeća.

• **Enterprise Console** – centralna konzola za upravljanje rešenjem, konfigurisanje polisa i rešavanje problema;

• **Patch Assessment** - Patch kontrolu krajnjeg korisnika u mreži za desetinu najpoznatijih softverskih proizvođača.

• **AutoUpdate** – omogućava sigurno ažuriranje i kontrolu protoka;   
  
• **Tamper Protection** - sprečavanje uklanjanja ili isključivanja Sophos bezbednosnog softvera od strane neautorizovanih korisnika ili softvera.

Licenca treba da uključi i potpuno funkcionalnu licencu za kućne korisnike zaposlene na Poljoprivrednom fakultetu u Novom Sadu.

Ponuđena cena treba da obuhvati:

• **Zakup prava na korišćenje softvera u dužini trajanja licence**

• **Obuku sistem administratora za administriranje Sophos proizvoda**. Obuka treba da obuhvati opšte upoznavanje sa aktuelnim internet pretnjama koje ugrožavaju kompanijske računarske mreže, administriranje Sophos Anti-Virus softvera kroz teoriju i praktične vežbe u laboratorijskom mrežnom okruženju, kao i uputstva za sprovođenje efektne antivirusne politike firme;

• **Tehničku podršku** u toku trajanja licenci.

• **Pravo na osvežavanje otisaka virusa i ostalog malicioznog koda u vreme trajanja licence** direktno sa Sophos-ovog web sajta.

• **Pravo na sve nove verzije softvera u toku trajanja licence.** Ne može biti dodatnih skrivenih troškova u slučaju izdavanja nove verzije softvera;

• **Licencu za kućno korišćenje antivirusnog softvera**