Република Србија
МИНИСТАРСТВО ПОЉОПРИВРЕДЕ,
ШУМАРСТВА И ВОДОПРИВРЕДЕ
Управа за ветерину
Број: 002032923 2025 14841 005 000 405 023
Датум: 26.06.2025. године
Београд

ПОЗИВ ЗА ПОДНОШЕЊЕ ПОНУДА

БЕОГРАД

Управа за ветерину – Министарства пољопривреде, шумарства и водопривреде, као Наручилац, покренула је поступак набавке лиценци за антивирусни софтвер за уређаје који сте користе у Управи за ветерину , те вас позивамо да доставите своју понуду до 03.07.2025. године до 10:00 часова, у складу са доле наведеним:

Понуђени антивирусни софтвер мора бити понуђен у последњој доступној комерцијалној верзији. Под комерцијалном верзијом софтвера Наручилац сматра последњу доступну комерцијалну (продајну) верзију софтвера , не тестну или развојну верзију софтвера коју произвођачи (у појединим случајевима) испоручују, али не обезбеђују уз испоручену верзију гаранцију по питању одржавања, ажурирања, као и по питању поузданости софтвера као што то чине у случају комерцијалних верзија.

Лиценце антивирусног програма за најмање 120 рачунара у трајању од 1 (једне) године са инсталацијом и подешавањем најновије верзије антивирусног програма.

Лиценце за коришћење и одржавање заштите од вируса и малициозних програма треба да буде јединствена, централно управљива и да обезбеди несметано коришћење софтвера према следећим техничким захтевима:

- мора да обухвати заштиту за оперативне системе Microsoft Windows 7/8/10/11, Microsoft Windows Server 2008/2012/R2/2016/2019/2022, Mac OS, Linux/FreeBSD, Android 6.x и новији, те да обезбеди централизовано управљање путем једне администраторске конзоле за све инстанце и модуле заштите;
- Мора да осигура заштиту Vmware виртуелног окружења и да подржава платформе Vmware NSX и vShield. Такође потребно је да решење подржава Vmware NSX automation, vMotion конзолом за даљинску администрацију, као и са Веб базираном конзолом. Да дозвољава такозвану „drill-down“ способност виртуелних машина за убрзано извршавање таскова и комплетан endpoint security management.
- Потребно је да решење подржава управљање и виртуелних и физичких машина са једне управљачке конзоле као да подржава могућност инсталације на више хостова одједном. Такође решење мора обезбедити оптимизовање ресурса и перформанси

тако да механизам за скенирање на злонамерне кодове не утиче битно на рад осталих апликација и процеса;

- Мора да обухвати могућност ефикасне заштите од малвера односно вируса, црва, тројанаца, адвер и спајвер софтвера, руткит-ова;
- Решење мора да поседује заштиту за мобилне уређаје на захтеваним платформама (mobile device management, mobile endpoint security, BYOD подршка) која је управљива путем јединствене централне конзоле из које се надгледају остале компоненте заштите на подржаним платформама и оперативним системима;
- Могућност контроле потенцијално нежељених апликација као што су IM, P2P, VoIP и сличних.
- Мора да обезбеди детекцију рањивости над протоколима као што су SMB, RPC, RDP и да омогући заштиту пре изласка званичне закрпе од стране произвођача софтвера и њене примене;
- Могућност спречавања извршавања дефинисане апликације на рачунару;
- Контролу и могућност блокирања одређених уређаја на радним станицама (CD/DVD, IrDA уређаји, уређаји повезани путем USB, Bluetooth i Firewire у складу са дефинисаном полисом (Device Control фукнционалност), као и могућност прикупљања лог фајлова са тих уређаја;
- Могућност заштите од тзв. „zero-day" претњи – проактивна заштита од познатих и непознатих претњи;
- Могућност провере рачунара у односу на низ правила и услова постављених од стране систем администратора и у односу на њихову испуњеност дозволи приступ рачунарској мрежи или смести рачунар у карантин (Network Access Control, NAC фукнционалност). NAC мора минимално да пружи могућност провере присутности и ажурираности антивирусног софтвера и да ли је примењен одговарајући „service pack" на оперативни систем рачунара;
- Могућност централизованог управљања и администрације решења, даљинске инсталације решења на клијентским и серверским машинама, као и Интернет приступ конзоли за надгледање и управљање заштитом. Конзола мора да омогући дефинисање различитих права приступа администраторима у зависности од политике наше организације;
- Могућност уклањања и дезинфекције претње даљинским путем са издвојене локације;
- Могућност централизованог ажурирања антивирусних и других дефиниција;
- Могућност праћења и извештавања о појави претњи и другим битним догађајима на систему као и акцијама које су уследиле након детекције претње или других догађаја;
- Могућност увоза група и корисника из Microsoft активног директоријума организације како би се на њих примениле полисе;
- Могућност аутоматског синхронизовања са активним директоријумом, где ће приликом детектовања новог рачунара који је члан домена он аутоматски бити увезен у конзолу за централизовано управљање и на њега ће се аутоматски применити дефинисана полиса за групу корисника којој припада;
- Могућност детаљног извештавања и креирања извештаја са могућношћу њиховог извожења у TXT, EVTX, PDF, XLS i CSV формат;

- Могућност за коришћење модула за Bootable System Recovery, као и медије за опоравак система приликом тежих инфекција;
- Могућност детекције малвера кроз скенирање HTTPS протокола и компримованих фајлова;
- Могућност дефинисања правила за системске регистре, процесе, апликације и фајлове, као и детекцију претњи на основу понашања система (Host Intrusion Prevention System, HIPS функционалност);
- Мора да поседује интегрисан алат за даљинско снимање слике процеса на клијентском рачунару (активни процеси, инсталирани софтвер, регистар база, мрежне конекције итд.) и уклањање тако уочених нежељених сервиса даљинским путем;
- Мора да обезбеди коришћење интегрисаног алата за креирање независних медија за чишћење и опоравак система у случају тежих инфекција малвером (SysRescue фукнционалност);
- Могућност праћења и обавештавања о променама на системским фајловима и апликацијама које приступају интернету (Application Modification Detection, AMD фукнционалност);
- Могућност самоодбране од малвера чија је намера да искључи заштиту на серверима или клијентским машинама;
- Могућност контроле Интернет саобраћаја на мрежи на основу дефинисаних Интернет полиса, интеграције са активним директоријумом и филтера за категоризацију садржаја;

Критеријум за оцењивање понуда је најнижа укупна цена.

Рок испоруке 30 (тридесет) дана од дана закључења

Чланом 27. став 1. тачка 1. Закона о јавним набавкама („Службени гласник РС“ број 91/19 и 92/23), прописано је да се одредбе овог закона не примењују се на набавку добара, услуга и спровођење конкурса за дизајн, чија је процењена вредност мања од 1.000.000 динара и набавку радова чија је процењена вредност мања од 3.000.000 динара.

Средства за реализацију набавке обезбеђена су Законом о буџету Републике Србије за 2025. годину („Службени гласник РС”, број 94/2024) раздео 24, глава 24.1, функција 760, економска класификација 515192, а наведена набавка се налази у интерном плану набавки Наручиоца за 2025. годину под редним бројем 2.2. набавке лиценци за антивирусни софтвер за уређаје који сте користе у Управи за ветерину.

Рок за подношење понуде је 03.07.2025. године до 10:00 сати.

Критеријум за избор најповољнијег понуђача јесте **најнижа укупна понуђена цена**.

С обзиром да Наручилац не користи електронски систем за спровођење изузетих набавки, а који закључава понуде у тренутку подношења тако да се могу откључати тек

непосредно по истеку рока за подношење истих, понуда не може бити достављена коришћењем електронске поште.

Понуђач понуду доставља препорученом поштом или личном предајом на писарници Управе за заједничке послове републичких органа, тако да буде запримљена до времена одређеног за отварање понуда, у затвореној коверти:

Управа за ветерину
Омладинских бригада бр. 1
Нови Београд

Напомена: за набавке лиценци за антивирусни софтвер за уређаје који сте користе у Управи за ветерину бр 002032923 2025 14841 005 000 405 023 :НЕ ОТВАРАТИ

Јавно отварање понуда биће извршено дана 03.07.2025. године са почетком у 10:15 сати, на адреси: Омладинских бригада бр.1, Нови Београд, I/52.

Оцена и рангирање понуда врши се на основу утврђеног критеријума, сачињава се извештај који садржи све основне податке о понуђачима, понуђеним ценама и другим траженим елементима понуде (цене, рокови, услови и начин плаћања, и сл.) и предлогом за закључење предметног уговора са најповољнијим понуђачем.

У овом поступку не доноси се посебна одлука о додели уговора, већ се уговор закључује на основу извештаја.

Марија Грбић,
службеник за јавне набавке
Управа за ветерину
Министарства пољопривреде,
шумарства и водопривреде

ПОДАЦИ О ПОНУЂАЧУ

ПОСЛОВНО ИМЕ ПОНУЂАЧА	

СЕДИШТЕ	**УЛИЦА И БРОЈ**	
	МЕСТО	
	ОПШТИНА	
МАТИЧНИ БРОЈ ПОНУЂАЧА		
ПОРЕСКИ БРОЈ ПОНУЂАЧА		
БРОЈ РАЧУНА И НАЗИВ БАНКЕ		
ЛИЦЕ ЗА КОНТАКТ		
ЕЛЕКТРОНСКА АДРЕСА ЛИЦА ЗА КОНТАКТ		
ТЕЛЕФОН		
ЛИЦЕ ОДГОВОРНО ЗА ПОТПИСИВАЊЕ УГОВОРА		

Место и датум

_____

Овлашћено лице понуђача

_____

ОБРАЗАЦ ПОНУДЕ

Број понуде и датум : _____

Укупна цена без ПДВ	_____динара без ПДВ
Укупна цена са ПДВ	_____динара са ПДВ

Рок важења понуде (минимум 30 дана од дана отварања понуда)	_____ дана од дана отварања понуда
Рок испоруке	_____дана од дана закључења уговора
Рок и начин плаћања:	Наручилац ће вршити плаћање, по пријему уредне е фактуре, на основу Записника о примопредаји предметних добара, на рачун изабраног понуђача/добављача, **у року од_____дана** (попуњава понуђач – за наручиоца је прихватљиво у року до 45 дана)

Место и датум

_____

Овлашћено лице понуђача

_____

Критеријум за избор најповољнијег понуђача јесте најнижа укупна понуђена цена услуга без ПДВ-а.

Уколико два понуђача понуде исту цену, уговор ће се доделити понуђачу који понуди дужи рок плаћања.

Напомене:

- Уколико понуђач није у систему ПДВ-а, понуђач ставља у понуди ту напомену.
- Наручилац није предвидео могућност повећања цене, те је понуђена цена коначна.
- **Приликом сачињавања понуде употреба печата није обавезна.**