Друштво за информациски решенија и услуги
АКСИАНС МАКЕДОНИЈА ДООЕЛ
Бр. 03-128/1
04.06 2025 год.
Скопје

Република Северна Македонија
Министерство за финансии

Архивски број: 03-62М/1-
Датум: 30-05-2025

ДОГОВОР
за јавна набавка на стоки – систем за периметарска заштита

Склучен помеѓу:

1. МИНИСТЕРСТВО ЗА ФИНАНСИИ, со седиште на ул.„Даме Груев“, бр.12 - Скопје, претставувано од м-р Гордана Димитриеска-Кочоска, министер за финансии, во натамошниот текст: договорен орган и
2. ДРУШТВО ЗА ИНФОРМАЦИСКИ РЕШЕНИЈА И УСЛУГИ АКСИАНС МАКЕДОНИЈА ДООЕЛ СКОПЈЕ, со седиште на ул.„Анкарска“ бр.31, 1000 Скопје, претставувано од Боро Антовски, управител, во понатамошниот текст: носител на набавката.

I. ПРЕДМЕТ НА ДОГОВОРОТ

Член 1

Предмет на договорот е јавна набавка на стоки – систем за периметарска заштита, согласно со техничките спецификации (Прилог 1 кон договорот) и понудата на носителот на набавката прифатена од страна на договорниот орган (Прилог 2 кон договорот), кои се составен дел од овој договор, а по претходно спроведена отворена постапка, по оглас број 04573/2025.

II. ВРЕДНОСТ НА ДОГОВОРОТ

Член 2

Вкупната вредност на договорот без пресметан данок на додадена вредност изнесува 6.795.025,00 денари.

Вкупниот износ на данок на додадена вредност изнесува 1.223.104,00 денари.

Вкупната вредност на договорот со пресметан данок на додадена вредност изнесува 8.018.129,00 денари.

III. РАЗЛИКА ВО ЦЕНА (КОРЕКЦИЈА НА ЦЕНИ)

Член 3

Цената од член 2 на овој договор е крајна, фиксна и непроменлива за цело времетраење на договорот.

IV. ВАЖНОСТ НА ДОГОВОРОТ

Член 4

Овој договор важи од денот на потпишување од двете договорни страни до истекот на претплатата на системот за периметарска заштита, која изнесува 2 (две) години сметано од денот на активирањето.

V. НАЧИН, МЕСТО И РОК НА ИСПОРАКА

Член 5

Предметот на договорт вклучува испорака, инсталација, конфигурација на систем за периметарска заштита, како и хардверска и софтверска претплата во период од 2 (две) години сметано од денот на целосната инсталација и ставање во употреба на системот, согласно со техничките спецификации кои се составен дел на тендерската документација.

Носителот на набавката е должен да го испорача, инсталира и конфигурира предметот на договорот во рок од 30 (триесет) дена од денот на приемот на писмена порачка од договорниот орган

За извршената испорака, инсталација и конфигурација договорните страни потпишуваат документ - работен налог или записник.

Работниот налог/Записник за извршената испорака со полно име и презиме ги потпишуваат определените лица од двете договорните страни, при што по еден примерок се предава на задолженото лице кај договорниот орган, еден примерок задржува носителот на набавката за сопствени потреби и еден примерок заедно со фактурата се доставува до Министерството за финансии - Скопје.

Местото на извршување на предметот на договорот е во Скопје на локацијата на Министерството за финансии на ул. „Даме Груев" бр.12.

За извршување на услугите – предмет на договорот, носителот на набавката ги вклучува лицата од стручниот кадар за извршување на набавката - предмет на договорот, согласно со прифатената понуда на носителот на набавката од страна на договорниот орган.

Министерство за финансии Република Северна Македонија | Ministria e Financave Republika e Maqedonisë së Veriut | Ул. „Даме Груев" бр.12, Скопје | Rr. „Dame Gruev" nr.12, Shkup | +389 2 3255 633 www.finance.gov.mk

Во исклучителни ситуации носителот на набавката може да изврши замена на лице од техничкиот персонал кој ќе учествува во извршувањето на договорот, со доставување на детално образложение и по добивање на одобрение од договорниот орган, под услов лицето да ги исполнува условите предвидени во потточка 2.4 од тендерската документација.

VI. НАЧИН И РОК НА ПЛАЌАЊЕ

Член 6

Договорниот орган плаќањето ќе го изврши во рок до 30 (триесет) дена од денот на доставувањето на фактурата за извршувањето на предметот на набавка во писарницата на Министерството за финансии.

Кон фактурата носителот на набавката задолжително доставува Работен налог/Записник кој мора да ги содржи податоците за извршувањето, потпишан од двете договорни страни и соодветен доказ/лог за извршената инсталација и конфигурација на системот во формат одобрен од договорниот орган, во спротивно фактурата нема да биде платена и ќе биде вратена на докомплетирање кај носителот на набавката.

Фактурата се доставува по пошта или лично во писарницата на Министерството за финансии, на ул.„Даме Груев" бр.12 во Скопје.

VII. ПРАВА И ОБВРСКИ НА НОСИТЕЛОТ НА НАБАВКАТА

Член 7

Носителот на набавката е должен своите обврски да ги извршува стручно, навремено и квалитетно, врз основа на барањата на договорниот орган дефинирани во техничките спецификации кои се составен дел од овој договор (Прилог 1 кон договорот) и понудата прифатена од договорниот орган (Прилог 2 кон договорот).

Носителот на набавката е должен да се придржува кон рокот за извршување на предметот на договорот, кој е дефиниран во член 5 став 2 од овој договор.

Носителот на набавката се обврзува предметната набавка да ја извршува со разумно знаење и внимание во согласност со професионалните стандарди и тековната легислатива која влијае на ваков предмет на набавка.

Носителот на набавката е должен веднаш по потпишување на договорот да му достави на договорниот орган податоци за лицата кои ќе бидат определени за реализација на договорот.

VIII. ПРАВА И ОБВРСКИ НА ДОГОВОРНИОТ ОРГАН

Член 8

Договорниот орган е должен да определи лица задолжени за реализација на договорот и за истото да го извести носителот на набавката.

Договорниот орган е должен да достави писмено барање (порачка) со точни спецификации и барања со цел да се изврши реализацијата на договорот.

Договорниот орган се обврзува дека плаќањето на носителот на набавката ќе го изврши во рокот од членот 6 на овој договор.

IX. ГАРАНЦИЈА ЗА КВАЛИТЕТНО И НАВРЕМЕНО ИЗВРШУВАЊЕ НА ДОГОВОРОТ

Член 9

Носителот на набавката е должен заедно со потпишаниот договор да достави банкарска гаранција за квалитетно и навремено извршување на договорот во висина од 5% од вкупната вредност на договорот со пресметан ДДВ.

Со банкарската гаранција за квалитетно и навремено извршување на договорот носителот на набавката безусловно гарантира за целосно, квалитетно и навремено извршување на обврските по овој договор.

Банкарската гаранција за квалитетно и навремено извршување на договорот треба да биде безусловна, неотповиклива и на прв повик наплатлива од страна на договорниот орган, треба да биде издадена од банка со седиште во Република Македонија или од странска банка.

Гаранцијата за квалитетно и навремено извршување на договорот ќе биде со важност до целосното реализирање на договорот.

Недоставување на банкарската гаранција претставува основ за раскинување на овој договор.

Договорниот орган се обврзува на носителот на набавката да му ја врати банкарската гаранција за квалитетно и навремено извршување на договорот во рок од 14 (четиринаесет) дена од денот на целосното реализирање на договорот.
Договорниот орган нема да ја врати банкарската гаранција за квалитетно и навремено извршување на договорот и ќе бара нејзино активирање од банката која ја има издадено, доколку предметната набавка не е реализирана според одредбите од договорот.

Во случај носителот на набавката поради непредвидени околности (виша сила или други оправдани причини) да не можел да ја изврши услугата,

договорниот орган нема да бара активирање на банкарската гаранција, доколку носителот на набавката достави писмено образложение до договорниот орган во кое ќе ги наведе причините за неизвршената или ненавремено извршената услуга, а образложението биде писмено прифатено од страна на договорниот орган.

X. ДОВЕРЛИВОСТ НА ПОДАТОЦИ И ИНФОРМАЦИИ

Член 10

Определените лица од носителот на набавката наведени во понудата за реализација на договорот, задолжително потпишуваат изјава за доверливост на информации и податоци непосредно пред извршувањето на услугата - предмет на договорот.

Под поимот информации и податоци се подразбираат сите внатрешни и надворешни документи, спецификации, лични податоци, истражувања на пазарот или податоци за него, финансиски или маркетиншки информации, други податоци или бизнис, оперативни или технички информации, како и сите останати податоци и информации и независно дали се дадени во писмена, вербална или електронска форма и се во сопственост на договорниот орган.

Исто така, поимот информации и податоци, ги опфаќа и сите други податоци кои не се сопственост на договорниот орган, а се користат за одредени цели во работните задачи и обврски. Тука спаѓаат податоци на сите партнери, клиенти, добавувачи или било кое правно или физичко лице кое со Договорниот орган има засновано деловен или било каков друг однос. Договорниот орган ги става податоците на располагање на носителот на набавката во врска со погоре наведената цел, а за непречено одвивање на работните задачи и обврски.

Член 11

Не се предмет на овој договор информации кои биле или станале јавно достапни, но не како резултат на откривање од страна на носителот на набавката и на договорниот орган и без да бидат прекршени одредбите на овој договор од страна на носителот на набавката што може да се докаже со писмена документација или за кои договорниот орган писмено потврдил дека се ослободени од обврска за неоткривање.

Член 12

Носителот на набавката под целосна морална, материјална и кривична одговорност, се обврзува за време на важноста на договорот и во период од (5) пет години од датумот на неговото истекување или раскинување да ги чува во тајност сите информации и податоци од било која област на договорниот орган, кои ќе му

Министерство за финансии Република Северна Македонија | Ministria e Financave Republika e Maqedonisë së Veriut | Ул. „Даме Груев" бр.12, Скопје | Rr. „Dame Gruev" nr.12, Shkup | +389 2 3255 633 | www.finance.gov.mk

бидат дадени во процесот на соработката и притоа нема да ги искористи истите за лични цели, во име на друго лице, ниту ќе ги даде на увид на трета страна.

Носителот на набавката се обврзува да ги чува во тајност сите документи и податоци кои содржат информации за договорниот орган или неговите активности, како и неговите односи со клиенти или трети лица, а кои биле подготвени или изнесени во врска со работата за која Носителот на набавката е ангажиран од страна на договорниот орган.

Член 13

Носителот на набавката може да ги открие кои било од информациите и податоците наведени во членот 10 став 2 и 3 заради постапување по писмено барање од страна на надлежен орган, со легитимна наредба врз основа на закон.

Носителот на набавката, пред да ги даде бараните податоци ќе се увери дека барањето е валидно и е во согласност со важечки закон и ќе ги открие ваквите податоци само до степен до кој тоа е барано од надлежниот орган кој има овластување да бара такво соопштување.

Член 14

За секој настан или сомневање во однос на закана за нарушување на доверливоста, интегритетот и расположливоста на податоците и информациите, носителот на набавката се обврзува веднаш писмено да го извести определеното лице кај договорниот органот.

Член 15

Носителот на набавката по писмено барање на договорниот орган веднаш ќе ги врати или уништи сите документи кои содржат податоци и информации за договорниот орган, а кои се добиени во врска со работата за која носителот на набавката е ангажиран од страна на договорниот орган, без задржување на било какви фотокопии, изводи или друг вид на копии од нив или дел од нив. И покрај уништувањето на било кој податок и материјали носителот на набавката ќе продолжи да се придржува кон неговата обврска од овој договор и други обврски кои произлегуваат од него, за чување во тајност на сите податоци и информации кои ги сознал на било кој начин, при исполнување на неговите обврски кои произлегуваат од овој договор.

Член 16

Објавувањето податоци, рекламирањето или публицитетот, како и прес конференциите направени од страна на носителот на набавката во однос на овој договор или вршење на заеднички деловни активности на договорните страни треба да бидат претходно одобрени од договорниот орган пред нивното спроведување.

Министерство за финансии Република Северна Македонија | Ministria e Financave Republika e Maqedonisë së Veriut | Ул. „Даме Груев“ бр.12, Скопје | Rr. „Dame Gruev" nr.12, Shkup | +389 2 3255 633 | www.finance.gov.mk

Член 17

Одредбите од глава X од овој договор се правно валидни и обврзувачки и кај сите вработени кај носителот на набавката кои имаат добиено овластување за користење на информациите и податоците кои се уредени со овој договор.

XI. УСЛОВИ ЗА РАСКИНУВАЊЕ НА ДОГОВОРОТ

Член 18

Овој договор може да се раскине спогодбено во согласност на двете договорни страни.

Член 19

Овој договор може да се раскине и едностранo поради непридржување или неисполнување на договорните обврски утврдени со овој договор.

Договорната страна која поради непридржување или неисполнување на договорните обврски го раскинува договорот, должна е тоа да и го соопшти на другата договорна страна без одлагање во писмена форма.

Договорот се смета за раскинат со денот на приемот на известувањето за раскинување на договорот.

Доколку дојде до раскинување на договорот поради неисполнување или ненавремено исполнување на обврските на договорот од страна на носителот на набавката, покрај наплата на банкарската гаранција носителот на набавката ќе биде одговорен за евентуалната штета што би ја предизвикал на договорниот орган како директна или индиректна последица на неговото работење.

Член 20

Кога една од договорните страни нема да ја исполни својата обврска, договорната страна може да бара исполнување на обврската од другата договорна страна или да го раскине договорот, а во секој случај има право на надомест на штетата.

Член 21

Кога договорната страна нема да ја исполни својата обврска во определениот рок, другата договорна страна може да и остави примерен дополнителен рок за исполнување на обврската.

Рокот од став 1 на овој член може да биде продолжен само по писмено барање на носителот на набавката и писмена согласност од договорниот орган.

Ако договорната страна која не ја исполнила својата обврска во определениот рок, не ја исполни обврската ни во дополнителниот рок, другата договорна страна може да го раскине договорот.

XII. ВИША СИЛА

Член 22

Ниту една од договорните страни нема да биде одговорна за неисполнување на обврските од овој договор до кое би дошло заради виша сила.

Под виша сила се подразбираат настани или околности на кои договорните страни не можат да влијаат и се надвор од нивната контрола, а го попречуваат нормалното извршување на договорот (елементарни непогоди, воени дејства, граѓански немири, штрајкови и сл.).

Вишата сила не вклучува настан што е предизвикан од небрежност или намерна активност што би предизвикала застој во извршувањето на обврските од договорот.

Ако една од договорните страни е спречена да ги исполнува своите обврски заради виша сила, должна е веднаш писмено да ја извести другата страна, со наведување на причините за вишата сила и по можност обезбедување на соодветен доказ.

За времетраењето на вишата сила сите права и обврски од овој договор мируваат.

Договорните страни се обврзуваат на ист начин да ја известат договорната страна за повторното воспоставување на нормални услови за извршување на договорот, односно за престанокот на дејството на вишата сила.

По отстранувањето на вишата сила договорот продолжува да се реализира.

XIII. ЗАВРШНИ ОДРЕДБИ

Член 23

Изменувања и дополнувања на договорот можат да се вршат со заедничка согласност на договорните страни по писмен пат.

Договорната страна која бара измена и/или дополнување на договорот е должна своето барање до другата страна да го достави во писмена форма.

Договорот може да се изменува и дополнува со анекс на договорот потпишан од двете договорни страни во согласност со Законот за јавните набавки.

Член 24

За сé што не е предвидено со овој договор, се применуваат одредбите од Законот за облигационите односи, Законот за јавните набавки и од другите позитивни прописи во Република Северна Македонија.

Член 25

Во случај на спор, договорните страни се согласни спорот да го решат спогодбено, а доколку во тоа не успеат, согласни се спорот да го решава предметно надлежниот суд во Скопје.

Член 26

Обработката на личните податоци при реализацијата на овој договор ќе биде во согласност со Законот за заштита на личните податоци.

Член 27

Овој договор е составен во 4 (четири) еднообразни примероци од кои 2 (два) примероци за договорниот орган и 2 (два) за носителот на набавката.

Договорен орган:	Носител на набавката:
РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА МИНИСТЕРСТВО ЗА ФИНАНСИИ СКОПЈЕ	ДРУШТВО ЗА ИНФОРМАЦИСКИ РЕШЕНИЈА И УСЛУГИ АКСИАНС МАКЕДОНИЈА ДООЕЛ СКОПЈЕ
м-р Гордана Димитриеска-Кочоска Министер за финансии	Боро Антовски Управител

Изработил: Петрина Мале
Контролирал: Даниела Јанкова
Одобрил: Татјана Васева
Проверил: м-р Маја Стаменковска Угриновска
Михајло Михајловски
Проверил: Андреј Ангеловски
Владимир Стојанов
Ирена Петковски
Согласен: д-р Андриана Матлиоска

Прилог 1 кон договор - Технички спецификации

Предметот на оваа јавна набавка е испорака, инсталација, конфигурација, како и хардверска и софтверска претплата во период од минимум 2 (две) години сметано од денот на целосната инсталација и ставање во употреба на системот за периметарска заштита.
Понудата треба да вклучува цена во која се вклучени сите трошоци за предметот на набавката, како и сите барани услуги, поправки, интервенции, замена на хардвер и резервни делови со сите вклучени давачки за време на гарантниот период.
Носителот на набавката е должен да го испорача, инсталира и конфигурира предметот на набавка во рок од 30 (триесет) дена од денот на приемот на писмена порачка од договорниот орган.

Предмет на оваа јавна набавка е следното:

Табела А

Уред за периметарска заштита **Количина: 2**	
Минимални технички карактеристики	
Достапност:	Решение кое што вклучува два безбедносни уреди за работа во високодостапен (HA) режим
Интерфејси:	• Минимум 8 x 10/100/1000 Base-T RJ-45 мрежни приклучоци • Минимум 2 x USB 3.0 порти; • Минимум 1 x конзолен RJ-45 мрежен приклучок; • Минимум 1 x менаџмент RJ-45 мрежен прикучок;
Проширливост:	Минимум 1 слободен слот наменет за дополнително проширување:
Работна меморија:	Минимум 16 GB RAM меморија со можност за проширување до минимум 64 GB со цел зголемување на бројот на истовремени конекции
Складирање на податоци и логови:	Интегриран SSD со капацитет од минимум 480 GB
Перформанси:	• Минимум пропусна моќ при целосна заштита од закани: 4,9 Gbps • Минимум пропусна моќ за NGFW заштита: 18,5 Gbps • Минимум пропусна моќ на IPS: 25,5 Gbps • Минимум пропусна моќ на огнен ѕид (1518B UDP): 79 Gbps • Минимум пропусна моќ за IPsec VPN (AES-128): 4,8 Gbps • Минимум пропусна моќ за HTTP/TLS инспекција при целосна заштита од закани: 2,9 Gbps

	• Минимум пропусна моќ за HTTP/TLS инспекција при IPS: 2,2 Gbps • Максимум доцнење на огнен ѕид: 10 милисекунди • Минимум 185.000 конекции во секунда • Минимум 2,7 милиони истовремени конекции
Виртуелизација и мрежна сегментација:	• Можност за креирање минимум 48 виртуелни инстанци за огнен ѕид; • Вклучени 2 виртуелни инстанци;
Димензија и инсталација:	1U Rack mountable – сите додатоци мора да бидат вклучени
Напојување:	Вклучено редундантно АС напојување
Огнен ѕид:	• Режим на работа во Layer 2 (transparent) и Layer 3 (routed);
	• Reverse-proxy функционалност;
	• Автентикација базирана на група на корисници;
	• Интеграција со Active Directory без инсталација на дополнителен агент на домен контролерот;
	• Можност за автентикација на корисници преку веб прелистувач за недоменски корисници;
	• Можност за Kerberos автентикација за single-sign-on;
	• Можност за креирање на виртуелни инстанци на огнен ѕид;
	• Распределување на филтри по политика;
IPsec VPN:	• Поддршка за Site-to-site IPsec VPN;
	• IKE Сертификат за автентикаија;
	• IPSec NAT Traversal;
	• Воспоставување на VPN во случај на динамички ИП адреси;
Оддалечен пристап:	• Оддалечен пристап за корисниците до локалната мрежа со користење на client и clientless VPN за најмалку 50 истовремени корисници
	• Моделот на лиценцирање мора да биде по принципот на број на истовремени корисници, а не по број на вкупни корисници
Превенција од упад:	• Минимум поддршка на следниве механизми на детекција: контрола на апликации, валидација на протоколи, базиран на однесување, потписи за искористување (exploit signatures);
	• Креирање на правила коишто овозможуваат изземање на мрежи (network exceptions) за IPS анализа на основа на: source и destination IP адреси, сервиси и/или комбинација на претходните три опции;
	• Детектира и блокира мрежни и напади на апликативно ниво, штитејќи ги минимум следниве сервиси: DNS, FTP, SNMP и Microsoft Windows сервиси;

	• Заштита од DNS Cache Poisoning и да ги заштити корисниците од пристап на блокираните доменски адреси;
	• Детекција и блокирање на апликации за далечинска контрола вклучувајќи ги и оние кои се во можност да прават тунелирање преку HTTP.
Контрола на Интернет апликации и URL страници:	• Препознавање на минимум 10.000 Интернет апликации
	• Препознавање и блокирање на апликации коишто се во можност да преват тунелирање преку HTTP;
	• Инспекција на HTTPS шифриран сообраќај во дојдовна и појдовна насока
	• Можност да користи правила за URL филтрирање со цел да му овозможи на администраторот грануларна контрола на HTTPS инспекцијата.
Препознавање и контрола на типот на содржина:	• Препознавање и контрола на типот на содржината што се испраќа односно презема
	• Треба да бидат поддржани минимум следниве типови на содржина:
	○ Архиви (zip, gzip, 7z, tar, jar, ace, RAR и WinRAR);
	○ Слики (jpeg, bmp, gif, png, tiff);
	○ Мултимедија (wmv, wma, avi, mp3, mp4, flv, mkv);
	○ Word (docx, odt, doc, rtf, one);
	○ Spreadsheet (xlsx, xls, ods);
	○ Presentation (pptx, ppt, odp, otp).
Мрежен Анти-вирус и Anti-bot заштита:	• Anti-bot мора да има можност за:
	○ детекција и блокирање на сомнително (малициозно) однесување во мрежата;
	○ скенирање на интерна мрежа со цел детекција на бот активности;
	• Анти-вирусот мора да има можност за:
	○ скенирање на архиви;
	○ блокирање пристап на злонамерни URL страници;
	○ инспекција на HTTPS шифриран сообраќај;
	○ скенирање на линкови (URLs) во електронска пошта.
Web Filtering:	• Блокирање по URL / Клучен збор / Фраза;
	• Листа на URL исклучоци;
	• Профили на содржина;
	• Блокирање на Java Applet, Active X;
	• Автоматско ажурирање на базата со веб страници.
Anti-spam заштита:	• Можност за детекција на појдовни и дојдовни спам e-mail пораки по следните критериуми:

	○ Содржина;
	○ Репутација на IP адреса;
	○ Листи за блокирање;
	○ Anti-Virus;
	○ IPS за заштита на e-mail.
Заштита од непознати злонамерни програми за коишто не постојат анти-вирусни дефиниции врз база на Sandbox решение:	• Zero-day заштита врз база на Cloud Sandbox технологија за закани кои доаѓаат по пат на: HTTP, HTTPS, FTP, SMTP и SMTP TLS сообраќај;
	• Решението мора да има можност за:
	○ Емулација на датотеки поголеми од 10MB;
	○ Скенирање на линкови во електронска пошта за zero-day напади т.е. непознати злонамерни програми;
	○ Отстранување на активни и потенцијално злонамерни делови од документот и безбедниот документ да го достави на крајниот корисник по пат на електронска пошта пред емулацијата, а истовремено да го прати оригиналниот документ - датотека на емулација;
	○ Преземање на оригиналниот документ ако истиот не е злонамерен од страна на корисник преку веб портал;
	○ За емулирање на извршни датотеки, архиви, документи, JAVA и Flash апликации, т.е. најмалку на следниве типови на датотеки: doc, docx, dot, dotm, dotx, exe, jar, pdf, potx, ppsx, ppt, pptm , pptx, rar, rtf, scr, swf, tar, xla, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, z ip, gz, cab, csv;
Лиценцирање:	• Сите барани безбедносни функционалности мора да бидат лиценцирани и активни за имплементација и работа.
	• Времетраење на лиценците: мин. 2 години
Гарантен рок и поддршка:	• Минимум 2 години гаранција на хардвер по принцип на испраќање исправен (заменски) уред истиот работен ден
	• Достапност на техничка поддршка од производителот 9 x 5 секој работен ден
	• Вклучени системски закрпи и адаптивно одржување
	• Пристап до база на знаење и техничка документација од производителот
	• Проактивен надзор на уредот од страна на производителот
	• Проактивната поддршка мора да обезбеди автоматско креирање на сервисно барање во случај на детекција на недостатоци на уредот
	• Ажурирање на дефиниции за сите типови закани

Табела Б

Поддршка и претплата	
Опис	Кол.
Support for Security Management Software – CPSM-NGSM5 Next Generation Security Management Software for 5 gateway Минимум 2 години	1
Annuity Blades for Management – CPSB-EVNT-5-1YCheck Point SmartEvent blade for Security Management for 5 gw – CPSB-RPRT-5-1YSmartReporter blade for Security Management for 5 gw Минимум 2 години	1

Во понудениот гарантен период од најмалку 2 (две) години носителот на набавката задолжително треба да обезбеди:

Техничка поддршка

Носителот на набавката треба да обезбеди:

- Адаптивно одржување на софтвер (Firmware, OS и др.) по потреба.
- Периодични проверки на состојбата на опремата користејќи ги достапните алатки за менаџмент како и проверка на логовите.
- Супервизија и контрола во случај на преместување на опремата на друга локација.
- Оптимизација на перформансите на опремата.
- Дизајн и консалтинг во случај на адаптивно одржување и промени на опремата.

Логистичка поддршка

Носителот на набавката треба да обезбеди:

- Замена на било кој неисправен дел од опремата во Табела А.
- Ако потребниот резервен дел не е поради било која причина на залиха, понудувачот треба да ја почне процедурата за нарачка на резервен дел следниот работен ден по пријавата на проблемот. Испораката на резервниот дел не треба да трае подолго од 30 денови по пријавата на проблемот.
- Администрација и плаќање на царински и шпедитерски давачки, даноци и други трошоци поврзани со испорака на резервните делови.

Одржување

Носителот на набавката треба да обезбеди:

- Проактивно решавање на проблемите со време на одзив од 4 часа.
- Еднаш месечно периодични превентивни мерки и прегледи (Health Check) на состојбата на опремата и софтверот кои вклучуваат:
  - Инспекција и визуелен преглед на хардверот за можни проблеми.
  - Анализа на перформанси и генерални проверки за состојбата на опремата.
  - Проверка на логовите на системите.
  - Проверка и тест на Alert-ти.
  - Генерирање dump file-ови од системот и негова анализа.
- Носителот на набавката во соработка со лицата за определени за реализација на набавката од договорниот орган ќе ги изведува сите потребни замени на неисправни делови, вклучувајќи ја и нивната физичка инсталација и конфигурација и ќе ја врати претходната функционалност на опремата.
- Реализација на барањата од договорниот орган за креирање и модификации на конфигурацијата на системот.

Обврски на носителот на набавката

- *Носителот на набавката во договорот треба да обезбеди:* Проактивно оддржување во согласност со условите дефинирани во ова барање.

Пријава на проблеми и време на одзив

Носителот на набавката во договорот треба:

- Да обезбеди јасна процедура за пријавување и ескалација на проблемите. Процедурата треба да понуди можности за пријавување по e-mail и телефон во зависност од сериозноста на проблемот.
- Времето на одзив е 4 часа од известувањето за постоење на проблем.

Понудувачот заедно со понудата задолжително треба да достави Технички опис на понудената ИКТ опремата со приложен проспектен материјал со референца во проспектниот материјал каде што може да се види бараната техничка карактеристика (Број на страна и маркиран текст во проспектниот материјал каде што може да се види бараната техничка карактеристика) и Овластување/ авторизација MAF (Manufacturer Authorisation Form) издадена од производителот на понудената опрема, каде треба да биде назначено името на авторизираниот понудувач (економски оператор) за ставките/стоките кои се бараат согласно техничката спецификација, во спротивно понудата ќе биде отфрлена како неприфатлива.

Прилог 2 кон договор

ОБРАЗЕЦ НА ПОНУДА

Врз основа на оглас објавен од страна на Министерството за финансии, за доделување на договор за јавна набавка на стоки – Систем за периметарска заштита, со спроведување на отворена постапка преку Електронскиот систем за јавни набавки (https://www.e-nabavki.gov.mk) и на тендерската документација ја поднесуваме следнава:

П О Н У Д А

Дел I – Информации за понудувачот

I.1. Име на понудувачот: **Аксианс Македонија ДООЕЛ**
I.2. Контакт информации:
-Адреса: **Анкарска 31, 1000 Скопје**
-Телефон: **02/3065396**
-Факс: **02/3065397**
-Е-пошта: **sales@axians.mk / marjan.asprovski@axians.mk**
-Лице за контакт: **Марјан Аспровски**
I.3. Одговорно лице: **Боро Антовски**
I.4. Даночен број: **МК4030994173880**
I.5. Матичен број на понудувачот: **4807804**
I.6. Согласни сме да ја дадеме оваа понуда за предметот на договорот за јавна набавка согласно со техничките спецификации.

Дел II – ТЕХНИЧКА ПОНУДА

II.1. Согласни сме да ви го обезбедиме предметот на набавка на Систем за периметарска заштита во се според барањата дефинирани во техничките спецификации кои се составен дел од тендерската документација.

Понудувачот заедно со понудата задолжително треба да достави Технички опис на понудената ИКТ опремата со приложен проспектен материјал со референца во проспектниот материјал каде што може да се види бараната техничка карактеристика (Број на страна и маркиран текст во проспектниот материјал каде што може да се види бараната техничка карактеристика) и **Овластување/ авторизација MAF (Manufacturer Authorisation Form) издадена од производителот на понудената опрема, каде треба да биде назначено името на авторизираниот понудувач (економски оператор) за ставките/стоките кои се бараат согласно техничката спецификација, во спротивно понудата ќе биде отфрлена како неприфатлива.**

Уред за периметарска заштита Количина: 2		**Понудено:2x Check Point Quantum Force 9100**
Минимални технички карактеристики		
Достапност:	Решение кое што вклучува два безбедносни уреди за работа во високодостапен (HA) режим	2x Check Point Quantum Force 9100 in High Availability Active/Active L2, Active/Passive L2 and L3 **Брошура: Check Point Quantum Force 9100.pdf стр: 4**

Интерфејси:	• Минимум 8 x 10/100/1000 Base-T RJ-45 мрежни приклучоци • Минимум 2 x USB 3.0 порти; • Минимум 1 x конзолен RJ-45 мрежен приклучок;	8x 10/100/1000 Base-T 2x USB 3.0 порти 2x USB 3.0 порти 1x RJ-45 Console Порт
	• Минимум 1 x менаџмент RJ-45 мрежен прикучок;	1x RJ-45 Management Порт **Брошура: Check Point Quantum Force 9100.pdf стр: 3, 5**
Проширливост:	Минимум 1 слободен слот наменет за дополнително проширување:	1x Expansion Slot **Брошура: Check Point Quantum Force 9100.pdf стр:3**
Работна меморија:	Минимум 16 GB RAM меморија со можност за проширување до минимум 64 GB со цел зголемување на бројот на истовремени конекции	16 GB RAM, можност за надградба до 64 GB memory **Брошура: Check Point Quantum Force 9100.pdf стр:3, 5**
Складирање на податоци и логови:	Интегриран SSD со капацитет од минимум 480 GB	1x 480 GB SSD SATA **Брошура: Check Point Quantum Force 9100.pdf стр:5**
Перформанси:	• Минимум пропусна моќ при целосна заштита од закани: 4,9 Gbps • Минимум пропусна моќ за NGFW заштита: 18,5 Gbps • Минимум пропусна моќ на IPS: 25,5 Gbps • Минимум пропусна моќ на огнен ѕид (1518B UDP): 79 Gbps • Минимум пропусна моќ за IPsec VPN (AES-128): 4,8 Gbps • Минимум пропусна моќ за HTTP/TLS инспекција при целосна заштита од закани: 2,9 Gbps • Минимум пропусна моќ за HTTP/TLS инспекција при IPS: 2,2 Gbps • Максимум доцнење на огнен ѕид: 10 милисекунди • Минимум 185.000 конекции во секунда • Минимум 2,7 милиони истовремени конекции	Threat Prevention: 4.95 Gbps NGFW: 18.6 Gbps IPS: 25.7 Gbps Firewall 1518B UDP (Gbps): 80 Gbps IPSec VPN AES-GCM 1452B: 22.1 Gbps HTTP/TLS Inspection Threat Prevention: 2.96 Gbps HTTP/TLS IPS: 2.3 Gbps Firewall Latency: 10µSec Connections/sec: 190,000 Concurrent connections: 2.75M **Брошура: Check Point Quantum Force 9100.pdf стр:3**
Виртуелизација и мрежна сегментација:	• Можност за креирање минимум 48 виртуелни инстанци за огнен ѕид; • Вклучени 2 виртуелни инстанци;	Maximum Firewall Virtual System Capacity: 48 The Base & Plus packages include 2 virtual systems (VS) **Брошура: Check Point Quantum Force 9100.pdf стр:4, 5**
Димензија и инсталација:	1U Rack mountable – сите додатоци мора да бидат вклучени	1U Rack Form Factor. **Брошура: Check Point Quantum Force 9100.pdf стр:2**

Напојување:	Вклучено редундантно AC напојување	2x Internal AC power supply **Брошура: Check Point Quantum Force 9100.pdf стр:3**
Огнен ѕид:	• Режим на работа во Layer 2 (transparent) и Layer 3 (routed);	Layer 2 (transparent) and Layer 3 (routing) mode **Брошура: Check Point Quantum Force 9100.pdf стр:4**
	• Reverse-proxy функционалност;	Reverse Proxy **Брошура: Check Point MobileAccess AdminGuide.pdf стр: 282**
	• Автентикација базирана на група на корисници;	Identiy of Users or user groups **Брошура: Check Point Quantum IdentityAwareness.pdf стр: 13**
	• Интеграција со Active Directory без инсталација на дополнителен агент на домен контролерот;	AD Query and Browser-Based Authentication, clientless employee access for all Active Directory Users **Брошура: Check Point Quantum IdentityAwareness.pdf стр: 100, 101**
	• Можност за автентикација на корисници преку веб прелистувач за недоменски корисници;	Browser-Based Authentication acquire identities from unidentified users (Unmanaged, guest users such as partners or contractors) **Брошура: Check Point Quantum IdentityAwareness.pdf стр: 103**
	• Можност за Kerberos автентикација за single-sign-on;	Transparent Kerberos Authentication Single-Sign On **Брошура: Check Point Quantum IdentityAwareness.pdf стр: 237**
	• Можност за креирање на виртуелни инстанци на огнен ѕид;	Virtual System Firewall: 48 qty **Брошура: Check Point Quantum Force 9100.pdf стр:4**
	• Распределување на филтри по политика;	Unified Access Control Policy for: • Firewall • Application and URL Filtering • Content Awareness • IPsec VPN and Mobile Access • Identity Awareness **Брошура: Check Point_Quantum SecurityManagement AdminGuide.pdf стр: 232**
IPsec VPN:	• Поддршка за Site-to-site IPsec VPN;	IPsec VPN Site-to- Site **Брошура: Check Point SitetoSiteVPN AdminGuide.pdf стр: 15 -17**
	• IKE Сертификат за автентикаија;	Public Key Infrastructure **Брошура: Check Point SitetoSiteVPN AdminGuide.pdf стр: 84-88**
	• IPSec NAT Traversal;	IPSec NAT Traversal **Брошура: Check Point SitetoSiteVPN AdminGuide.pdf стр: 184-185**

	• Воспоставување на VPN во случај на динамички ИП адреси;	VPN Routing for Security Gateways in SmartConsole with dynamically assigned IP addresses **Брошура: Check Point SitetoSiteVPN AdminGuide.pdf стр: 104**
Оддалечен пристап:	• Оддалечен пристап за корисниците до локалната мрежа со користење на client и clientless VPN за најмалку 50 истовремени корисници	Mobile Access Blade for 50 concurrent connections **Брошура: Check Point VPN License Guide.pdf стр. 1**
	• Моделот на лиценцирање мора да биде по принципот на број на истовремени корисници, а не по број на вкупни корисници	Mobile Access: This license is enforced based on concurrent connections **Брошура: Check Point VPN License Guide.pdf стр. 2**
Превенција од упад:	• Минимум поддршка на следниве механизми на детекција: контрола на апликации, валидација на протоколи, базиран на однесување, потписи за искористување (exploit signatures);	Checkpoint defense in depth approach combines signatures, protocol validation, anomaly detection, behavioral analysis, and other methods to provide the highest levels of network IPS protection **Брошура: Check Point_IPS.pdf стр: 1**
	• Креирање на правила коишто овозможуваат изземање на мрежи (network exceptions) за IPS анализа на основа на: source и destination IP адреси, сервиси и/или комбинација	Threat Prevention Profile and Rules, The Threat Prevention page shows the rules and exceptions for the Threat Prevention policy. The rules set the Threat profiles for the network objects or locations defined as a protected
	на претходните три опции;	scope **Брошура: Check Point ThreatPrevention AminGuide.pdf стр: 58**
	• Детектира и блокира мрежни и напади на апликативно ниво, штитејќи ги минимум следниве сервиси: DNS, FTP, SNMP и Microsoft Windows сервиси;	The Protocol Parsers main functions are to ensure compliance to well-defined protocol standards, detect anomalies if any exist, and assemble the data for further inspection by other components of the IPS engine. They include HTTP, SMTP, DNS, IMAP, SNMP, FTP and others **Брошура: Check Point ATRG IPS.pdf стр: 5-8**
	• Заштита од DNS Cache Poisoning и да ги заштити корисниците од пристап на блокираните доменски адреси;	DNS Server Protections **Брошура: Check Point DNS Protection SmartConsole R80.20 Help.pdf стр:1**
	• Детекција и блокирање на апликации за далечинска контрола вклучувајќи ги и оние кои се во можност да прават тунелирање преку HTTP.	IPS Detection and prevention of protocol misuse which in many cases indicates malicious activity or potential threat. Examples of commonly manipulated protocols are HTTP, SMTP, POP, and IMAP **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 26**
Контрола на Интернет апликации и URL страници:	• Препознавање на минимум 10.000 Интернет апликации	More than 10000 Applications **https://appwiki.checkpoint.com/appwikisdb/public.htm**
	• Препознавање и блокирање на апликации коишто се во можност да преват тунелирање преку HTTP;	HTTPS Inspection on Non-Standard Ports **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 372**

	• Инспекција на HTTPS шифриран сообраќај во дојдовна и појдовна насока	HTTPs Inspection • Outbound HTTPS Inspection - To protect against malicious traffic that is sent from an internal client to an external site or server. • nbound HTTPS Inspection - To protect internal servers from malicious requests that arrive from the Internet or an external network. **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 354-363**
	• Можност да користи правила за URL филтрирање со цел да му овозможи на администраторот грануларна контрол а на HTTPS инспекцијата.	HTTPS Inspection Policy The HTTPS Inspection rules can use the URL Filtering categories to identify traffic for different websites and applications. For example, to protect the privacy of your users, you can use a rule to ignore HTTPS traffic to banks and financial institutions **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 364-365**
Препознавање и контрола на типот на содржина:	• Препознавање и контрола на типот на содржината што се испраќа односно презема	Content Awareness (CTNT) is a new blade introduced in R80.10 as part of the new Unified Access Control Policy. Using Content Awareness blade as part of Firewall policy allows the administrator to enforce the Security Policy based on the content of the traffic by identifying files and its content **Брошура: Check Point ATRG Content Awareness (CTNT).pdf стр: 1**
	• Треба да бидат поддржани минимум следниве типови на содржина:	

	○ Архиви (zip, gzip, 7z, tar, jar, ace, RAR и WinRAR);	zip, gzip, 7z, tar, jar, ace, RAR и WinRAR **Брошура: Check Point Supported file types in Content Awareness Software Blade R80 and higher.pdf**
	○ Слики (jpeg, bmp, gif, png, tiff);	jpeg, bmp, gif, png, tiff **Брошура: Check Point Supported file types in Content Awareness Software Blade R80 and higher.pdf**
	○ Мултимедија (wmv, wma, avi, mp3, mp4, flv, mkv);	wmv, wma, avi, mp3, mp4, flv, mkv **Брошура: Check Point Supported file types in Content Awareness Software Blade R80 and higher.pdf**
	○ Word (docx, odt, doc, rtf, one);	docx, odt, doc, rtf, one **Брошура: Check Point Supported file types in Content Awareness Software Blade R80 and higher.pdf**
	○ Spreadsheet (xlsx, xls, ods);	xlsx, xls, ods **Брошура: Check Point Supported file types in Content Awareness Software Blade R80 and higher.pdf**

	○ Presentation (pptx, ppt, odp, otp).	pptx, ppt, odp, otp **Брошура: Check Point Supported file types in Content Awareness Software Blade R80 and higher.pdf**
Мрежен Анти-вирус и Anti-bot заштита:	• Anti-bot мора да има можност за:	
	○ детекција и блокирање на сомнително (малициозно) однесување во мрежата;	Anti-Bot Software Blade • Identify the C&C addresses used by criminals to control bots • Identify the communication patterns used by each botnet family • Identify bot behavior **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 27-28**
	○ скенирање на интерна мрежа со цел детекција на бот активности;	THREATSPECT™BOT DISCOVERY ENGINE Bots are stealthy, often hiding in your computer undetectable by common antivirus programs. The Check Point Anti-Bot Software Blade detects bot-infected machines with its ThreatSpect™ engine, a unique multi-layer discovery technology with up-tothe-minute updates feeds from ThreatCloud. ThreatSpect correlates information for accurate bot detection **Брошура: Check Point Anti-bot.pdf стр: 1**
	• Анти-вирусот мора да има можност за:	
	○ скенирање на архиви;	Enabling Archive Scanning You can configure the Anti-Virus settings to enable archive scanning. The Anti-Virus engine unpacks archives and applies proactive heuristics. The use of this feature impacts network performance. **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 88**
	○ блокирање пристап на злонамерни URL страници;	Anti-Virus: Accessed URLs are checked by the gateway caching mechanisms or sent to the ThreatCloud repository to determine if they are permissible or not. If not,
		the attempt is stopped before any damage can take place **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 28-29**
	○ инспекција на HTTPS шифриран сообраќај;	HTTPS Inspection Policy **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 364**
	○ скенирање на линкови (URLs) во електронска пошта.	Inspection of Links Inside Mail **Брошура: Check Point Links Inside Mails.pdf стр: 1**

Web Filtering:	• Блокирање по URL / Клучен збор / Фраза;	Custom Applications/Sites for Application Control and URL Filtering **Брошура Check Point Custom Applications_Sites for Application Control and URL Filtering.pdf стр: 1-2**
	• Листа на URL исклучоци;	HTTPs Validation: Whitelisting **Брошура: Check Point_Quantum SecurityManagement AdminGuide.pdf стр: 435**
	• Профили на содржина;	Working with Policy Packages: Access Control & HTTPS Inspection **Брошура: Check Point_Quantum SecurityManagement AdminGuide.pdf стр: 227**
	• Блокирање на Java Applet, Active X;	Secure Configuration Verification, Secure Configuration Verification **Брошура: Check Point RemoteAccessVPN AdminGuide.pdf стр: 91**
	• Автоматско ажурирање на базата со веб страници.	URL Filtering, The new URL Filtering software blade uses a hosted categorization service (cloudbased categorization) that is being constantly updated to cope with the dynamic nature of the web **Брошура: Check Point ATRG URL Filtering.pdf стр:10**
Anti-spam заштита:	• Можност за детекција на појдовни и дојдовни спам e-mail пораки по следните критериуми:	
	○ Содржина;	Content based AntiSpam **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 343**
	○ Репутација на IP адреса;	IP Reputation AntiSpam **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 343**
	○ Листи за блокирање;	Block List Anti-Spam **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 343**
	○ Anti-Virus;	Mail Anti-Virus **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 343**
	○ IPS за заштита на e-mail.	IPS **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 343**
Заштита од непознати злонамерни програми за коишто не постојат анти-	• Zero-day заштита врз база на Cloud Sandbox технологија за закани кои доаѓаат по пат на: HTTP, HTTPS, FTP, SMTP и SMTP TLS сообраќај;	SandBlast Zero-Day Threats: Supported Protocols: HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel, FTP **Брошура: Check Point Sandblast network solution brief.pdf стр:7**
вирусни дефиниции врз база	• Решението мора да има можност за:	

на Sandbox решение :	○ Емулација на датотеки поголеми од 10MB;	Emulation Limits: Maximum file size (up to 100,000 KB **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 314**
	○ Скенирање на линкови во електронска пошта за zero-day напади т.е. непознати злонамерни програми;	SandBlast Network protects users against these threats, using Threat Extraction to eliminate risk from all incoming email, as well as vetting all aspects of email messages before they enter your users' mailbox, including email attachments, email links, sender and recipient details and the text within **Брошура: Check Point Sandblast network solution brief.pdf стр:3**
	○ Отстранување на активни и потенцијално злонамерни делови од документот и безбедниот документ да го достави на крајниот корисник по пат на електронска пошта пред емулацијата, а истовремено да го прати оригиналниот документ - датотека на емулација;	SandBlast Threat Extraction promptly delivers clean and reconstructed versions of potentially malicious files that are received by email or downloaded from the web **Брошура: Check Point Sandblast network solution brief.pdf стр:3**
	○ Преземање на оригиналниот документ ако истиот не е злонамерен од страна на корисник преку веб портал;	Threat Extraction General Settings; Allow the user to access the original file **Брошура: Check Point ThreatPrevention AdminGuide.pdf стр: 115** **Брошура: Check Point Sandblast network solution brief.pdf стр:3**
	○ За емулирање на извршни датотеки, архиви, документи, JAVA и Flash апликации, т.е. најмалку на следниве типови на датотеки: doc, docx, dot, dotm, dotx, ex e, jar, pdf, potx, ppsx, ppt, pptm, pptx, r ar, rtf, scr, swf, tar, xla, xls, xlsb, xlsm, xl sx, xlt, xltm, xltx, xlw, zip, gz, cab, csv;	Supported File Types: doc, docx, dot, dotm, dotx, exe, jar, pdf, potx, pps x, ppt, pptm, pptx, rar, rtf, scr, swf, tar, xla, xls, xls b, xlsm, xlsx, xlt, xltm, xltx, xlw, zip, gz, cab, csv; **Брошура: Check Point File types supported by Threat Emulation.pdf стр: 1-5**
Лиценцирање:	• Сите барани безбедносни функционалности мора да бидат лиценцирани и активни за имплементација и работа.	9100 Base Appliance with SandBlast subscription package for 2 year; Next Generation Threat Prevention and Sandblast for additional 2 year for 9100 Base Appliance; Mobile Access Blade for 50 concurrent connections for 2 Year for 9100 Base Appliance;
	• Времетраење на лиценците: мин. 2 години	9100 Base Appliance with SandBlast subscription package for 2 year; Next Generation Threat Prevention and Sandblast for additional 2 year for 9100 Base Appliance; Mobile Access Blade for 50 concurrent connections for 2 Year for 9100 Base Appliance;
Гарантен рок и поддршка:	• Минимум 2 години гаранција на хардвер по принцип на испраќање исправен (заменски) уред истиот работен ден	2 години гаранција на хардвер по принцип на испраќање исправен (заменски) уред истиот работен ден

	• Достапност на техничка поддршка од производителот 9 x 5 секој работен ден	Достапност на техничка поддршка од производителот 9 x 5 секој работен ден
	• Вклучени системски закрпи и адаптивно одржување	Вклучени системски закрпи и адаптивно одржување
	• Пристап до база на знаење и техничка документација од производителот	Пристап до база на знаење и техничка документација од производителот
	• Проактивен надзор на уредот од страна на производителот	Проактивен надзор на уредот од страна на производителот
	• Проактивната поддршка мора да обезбеди автоматско креирање на сервисно барање во случај на детекција на недостатоци на уредот	Проактивната поддршка мора да обезбеди автоматско креирање на сервисно барање во случај на детекција на недостатоци на уредот
	• Ажурирање на дефиниции за сите типови закани	Ажурирање на дефиниции за сите типови закани

Табела 2

Поддршка и претплата		**Понудено:**
Опис	**Кол.**	
Support for Security Management Software – **CPSM-NGSM5** Next Generation Security Management Software for 5 gateway Минимум 2 години	1	**CPSM-NGSM5** Next Generation Security Management Software for 5 gateways 2 години
Annuity Blades for Management – **CPSB-EVNT-5-1Y**Check Point SmartEvent blade for Security Management for 5 gw – **CPSB-RPRT-5-1Y**SmartReporter blade for Security Management for 5 gw Минимум 2 години	1	**CPSB-EVNT-5-1Y**Check Point SmartEvent blade for Security Management for 5 gw **CPSB-RPRT-5-1Y** SmartReporter blade for Security Management for 5 gw 2 години

НАПОМЕНА: Задолжително да се пополнат празните колони во табелите во спротивно понудата ќе се отфрли како неприфатива.

Дел III - ФИНАНСИСКА ПОНУДА

III.1. Вкупната цена на нашата понуда, вклучувајќи ги сите трошоци и попусти, без ДДВ, изнесува: **6.795.025,00** *[со бројки]* (**шестмилиониседумстотинидеведесетипетилјадидваесеипетденари**) *[со букви]* денари.

Вкупниот износ на ДДВ изнесува **1.223.104,50** [*со бројки*] (**еденмилиондвестедваесетитриилјадистоичетириденариипедесетдени**) [*со букви*] денари.

III.2. Нашата понуда важи за периодот утврден во тендерската документација.

III.3. Се согласуваме со начинот и рокот на плаќање утврден во тендерската документација.

III.4. Ги прифаќаме начинот, местото и рокот за испорака на предметната стока, наведени во тендерската документација.

III.5. Со поднесување на оваа понуда, во целост ги прифаќаме условите предвидени во тендерската документација и не го оспоруваме Вашето право да ја поништите постапката за доделување на договор за јавна набавка согласно со член 114 од Законот за јавните набавки.

Дел IV - СОСТАВНИ ДЕЛОВИ НА ПОНУДАТА:

IV.1. Нашата понуда е составена од следниве делови:

- пополнет образец на понуда;
- докази дека нема причини за исклучување од постапката од точка 2.2.2 од тендерската документација;
- документи за утврдување на способноста за вршење на професионална дејност наведени во точка 2.3.1 од тендерската документација;
- документи за утврдување на техничка и професионална способност наведени во точка 2.4 од тендерската документација;
- сертификати за управување на квалитет наведени во точка 2.5 од тендерската документација;
- Технички опис на понудената ИКТ опремата и Овластување/ авторизација MAF (Manufacturer Authorisation Form) издадена од производителот на понудената опрема (согласно погоренаведеното;
- изјава за сериозност на понудата.

Место и датум	Овластено лице
Скопје, 14.04.2025	**Јован Поповски**
	(потпис*)

**Овој образец не се потпишува своерачно, туку исклучиво електронски со прикачување на валиден дигитален сертификат чиј носител е одговорното лице или лице овластено од него.*
***НАПОМЕНА: Доколку понудувачот понудата ја поднесува како група понудувачи, со подизведувач, користи способност од друг субјект или има доверливи информации, понудувачот во прилог на понудата ги доставува и другите барани прилози кон тендерската документација.*