ДОГОВОР

за набавка на централен систем за управување со антивирусна заштита и антивирусна заштита (сервери, персонални компјутери), анти спам заштита за електронски поштенски сандачиња во Microsoft Ex-change Server

ДОГОВОРНИ СТРАНИ

1. **Министерство за труд и социјална политика**, со седиште на ул.„Даме Груев„ бр.14 Скопје, претставувано од Министер **Јованка Тренчевска**, во понатамошниот текст: Нарачувач, и
2. **Друштво за комуникациски услуги А1 МАКЕДОНИЈА ДООЕЛ,Скопје**, ЕМБС 7068310,со седиште на Плоштад Пресвета Богородица бр.1 Скопје, претставуван од управителот Јиржи Дворјанчански и управител Иван Скендер, а преку овластено лице Стевчо Ристески, директор на бизнис и ИКТ продажба (во понатамошен текст Носител на набавката).

ПРЕДМЕТ НА ДОГОВОРОТ

Член 1

Со овој договор се уредуваат меѓусебните права и обврски помеѓу Договорниот орган и Носителот на набавката, согласно спроведената постапка за јавна набавка како постапка од мала вредност за услуги во согласност со позитивните законски прописи поврзани со предметот на набавката (Законот за јавни набавки , Законот за облигациони односи и други важечки прописи) кои се во сила во моментот на склучување на овој Договор .

Договорните страни го склучуваат овој договор врз основа на Одлука за јавна набавка со архивски број 02-6566/1 од 16.09.2022 година , одлука за избор за најповолен понудувач донесена во истата постапка, како и врз основа на доставена понуда од Носителот на набавката со која во целост се прифатени условите , барањата и напомените предвидени во тендерската документација .

Предмет на овој договор е **за набавка на централен систем за управување со антивирусна заштита и антивирусна заштита (сервери, персонални компјутери), анти спам заштита за електронски поштенски сандачиња во Microsoft Ex-change Server за период од две години**.

Антивирусната заштита на ИКТ опремата во Министерството за труд и социјална политика, ЦСР и Јавните социјални установи е една од најбитните алатки за обезбедување на доверливост и безбедност на податоците во ИКТ опремата (компјутери и сервери). Анти-спам заштитата на системот за размена на електронска пошта е најбитната алатка за одржување на хигиената на електронската пошта.

ЈАЗИК НА ДОГОВОРОТ

Член 2

Јазик на Договорот и на другите документи кои претставуваат составен дел на Договорот е македонскиот јазик.

Јазик на целата комуникација во писмена форма помеѓу договорните страни е на македонски јазик.

ВРЕДНОСТ НА ДОГОВОРОТ

Член 3

Вкупната вредност на овој договор изнесува **2.631.350,00** денари без пресметан данок на додадена вредност.

Вкупната цена на набавка со пресметан данок на додадена вредност изнесува **2.762.917,50** денари.

Поединечните цени се дадени во продолжение на овој Договор

Реден број	**Опис**	**Единечна мерка**	**Количина**	**Единечна цена без ддв**	**Вкупна цена со ддв**
1	Антивирусна заштита за сервери	лиценца	25 сервери (виртуелни или физички)	1.300,00	34.125,00
2	Антивирусна заштита за работни станици (персонални компјутери)	лиценца	1353	1.300,00	1.846.845,00
3	Централен систем за управување со антивирусната заштита	лиценца	1	6.000,00	6.300,00
4	Анти-спам заштита за електронски поштенски сандачиња во Microsoft Exchange Server	лиценца	1283 електронски поштенски сандачиња	650,00	875.647,50
	Вкупно без вклучен ддв			**2.631.350,00**	
	ДДВ			**131.567,50**	
	Вкупно со ддв			**2.762.917,50**	

НАЧИН, УСЛОВИ И РОК НА ИСПОРАКА

Член 4

Носителот на набавката е должен да го извршува договорот по барање на одговорно лице за реализација на овој предмет на јавна набавка кај Договорниот орган.

Носителот на набавката е должен да обезбеди антивирусна заштита во рок не подолг од 50 (педесет) календарски дена, сметајќи од денот на нарачка доставена од овластено лице за реализација на договорот кај Договорниот орган.

ВРЕМЕТРАЕЊЕ НА ДОГОВОРОТ

Член 5

Договорот е со важност од 2 (две) години,сметано од моментот на потпишување на двете договорни страни .

НАЧИН, УСЛОВИ И РОКОВИ НА ПЛАЌАЊЕ

Член 6

Начин на плаќање е во рок од 60 дена од денот по приемот на фактурата со прилог писмена нарачка за извршена испорака – предмет на договорот во Архивата на Министерството за труд и социјална политика.

Член 7

При изготвувањето на фактурата, Носителот на набавката е должен да ги наведе следните елементи:

- повикување на број на договорот;
- датум на изготвување на фактурата;
- количини со опис на опремата дефинирана по позиции онака како што се опишани во техничката спецификација;
- единечни договорени цени за секоја од позициите без вкалкулиран ДДВ;
- вкупни цени по позиции без вкалкулиран ДДВ;
- вкупна цена на фактурата;
- пресметка на данокот за додадена вредност;
- вкупна цена за исплата по фактурата (доколку имало евентуално намалување);
- валута на плаќање;
- рок на плаќање; и

сметка и банка на давателот на фактурата

Некомплетно доставена ф-ра од страна на носителот на набавката, договорниот орган/одговорно лице за реализација на договорот ќе ја врати писмено во кое ќе биде образложена причината за враќањето и рокот во кој носителот на набавката е должен да ги исправи недостатоците или грешките. Доколку носителот на набавката не достави ф-ра согласно насоките и не ги исправи недостатоците или грешките, рокот за плаќање ќе започне да тече од денот на постапувањето по укажувањето и приемот во архивата на изготвена ф-ра согласно овој член од договорот.

ГАРАНЦИЈА ЗА ИЗВРШУВАЊЕ НА ДОГОВОРОТ

Член 8

Навременото и квалитетно извршување на договорот, носителот на набавката го гарантира со доставување безусловна банкарска гаранција од банка прифатлива за договорниот орган.

Висината на банкарската гаранција изнесува *10%* од вкупната вредност на договорот.

Гаранцијата за квалитетно извршување на договорот ќе биде наплатена доколку носителот на набавката не исполни некоја од обврските од договорот за јавна набавка во рокот на стасаноста, за што писмено ќе го извести носителот на набавката.

Оваа гаранција се враќа на носителот на набавката, во рок од 14 дена од денот на целосно реализирање на договорот.

Во случај кога е продолжен рокот за реализација на договорот или е зголемена неговата вредност, носителот на набавката соодветно треба да ја продолжи важноста и вредноста на гаранцијата за квалитетно и навремено извршување на договорот.

ОБВРСКИ НА НОСИТЕЛОТ НА НАБАВКАТА

Член 9

Носителот на набавката е должен совесно,квалитетно и професионално да ја испорача стоката за набавка на централен систем за управување со антивирусна заштита и антивирусна заштита (сервери, персонални компјутери), анти спам заштита за електронски поштенски сандачиња во Microsoft Ex-change Server.

Член 10

Антивирусната заштита треба да може да се инсталира и да работи на работни станици (персонални компјутери)соWindows 11 Pro, Windows 11 Pro for Workstations, Windows 11 Enterprise, Windows 10 Pro, Windows 10 Pro for Workstations, Windows 10 Enterprise, и сервери (Microsoft Windows Server 2012, 2016, 2019, 2022).

Ред. Бр.	Барања за антивирусна заштита
1	Антивирусната заштита треба да заштитува од вируси, rootkit-ови, malware-и.
2	Со антивирусната заштита треба може да се управува со апликации вклучувајќи и нивна забрана.
3	Антивирусната заштита треба да заштитува од интернет прелистувачки базирани злоупотреби, интернет закани...
4	Антивирусната заштита треба да го заштитуваперсоналниот компјутер во

	реално време.
5	Антивирусната заштита треба да може да ги спречи обидите на малициозните програми да ја онеспособат антивирусната заштита.
6	Антивирусната заштита треба да може активно да блокира неавторизираните обиди за модификација на оперативниот систем или други апликации.
7	Антивирусната заштита треба да може да ги заштитува од инфекција од преносни носачи на податоци, како на пример USB мемории, CD и DVD.
8	Антивирусната заштита треба да може да употреби локален и/или далечински сервер за ажурирање/апдејтување на базни дефиниции за нови вируси.
9	Антивирусната заштита треба биде локациска "свесна" (во случај персоналниот компјутер да е надвор од корпоративната мрежа да употреби посебна полиса за update на дефиниции и заштита).
10	Антивирусната заштита треба има вграден персонален огнен ѕид.
11	Антивирусната заштита треба може да се интегрира со Microsoft Active Directory.
12	Антивирусната заштита треба има заштита од zero day напади.
13	Антивирусната заштита треба вклучува и Host-Level Intrusion Prevention System (HIPS) заштита.
14	Антивирусната заштита треба да може да се инсталира на персонален компјутер од далечина.
15	Антивирусната заштита треба да овозможи регулација на распоредувањето на ресурсите помеѓу антивирусната заштита и другите програми во зависност од приоритетот на задачите: опција за продолжување на скенирањето на антивирусната заштита во позадина.
16	Антивирусната заштита треба да има можност за работа во таканаречен lightweight мод на работа кој нуди намалено искористување на оперативна меморија, процесорско време и дисков простор на персоналниот компјутер, при што антивирусните дефиниции се преземаат во реално време од cloud сервис на производителот на антивирусната заштита, без претходно нивно запишување на диск.
17	Антивирусната заштита треба да има функционалност за заштита на персоналниот компјутер од кражби: комплетно блокирање на уредот, бришење на приватните податоци, пораки и контакт листи, лоцирање на уредот. Сето ова треба да се врши далечински, преку централната конзола за менаџирање. Решението треба да вклучува опции против кражба "Anti-theft" со кои треба да се минимизираат ризиците од прекршување на безбедноста кои можат да резултираат од изгубен или украден уред.

18	Антивирусната заштита треба да поддржува инсталација на антивирусната заштита на персоналните компјутери преку следниве методи: далечински преку RPC, GPO и мрежни агенти, илокално преку креирање на самостојни инсталациски пакети.
19	Антивирусната заштита треба да овозможува ограничување на пристап до надворешни USB мемории, CD, DVD и други уреди за складирање на податоци, способност да креира доверливи уреди по идентификатор и креирање дозвола само на одредени корисници да пристапат до тие уреди.
20	Антивирусната заштита треба да има можност за запишување на трансакциите на датотеките од и кон надворешни уреди.
21	Антивирусната заштита треба да има можност за импорт/експорт на листа на доверливи уреди во .xml формат.
22	Од антивирусната заштита треба да може да се извезат извештаи минимум во PDFформат.
23	Антивирусната заштита треба да може да направи проверка и дезинфекција на датотеки спакувани со програми како LZEXE, PKLITE, EXEPACK, DIET или еквивалентни.
24	Антивирусната заштита треба да овозможува антивирусна проверка и дезинфекција на датотеки минимум архивирани во LHA, RAR, ARJ, ZIP,JAR, CAB, ICE или еквивалентни формати, вклучувајќи ги и датотеките заштитени со лозинка.
25	Антивирусната заштита треба да може да скенираскрипти, даги скенирасите скрипти, минимум развиени преку Microsoft Internet Explorer (JavaScript, Visual Basic Script WSH scripts) или еквивалентни, кои се подигаат кога корисникот работи на компјутер или е на интернет.
26	Антивирусната заштита треба да има интегрирана компонента за заштита од криптовируси (ransomware) со можност за анализирање на активностите на програмите и процесите, спречување на активности поврзани со енкриптирање на податоци и враќање на backup копија од датотеката при обид за енкрипција.
27	Антивирусната заштита треба да има можност за инсталација на посебна алатка за заштита од криптовируси (ransomware) на уреди на кои не е инсталирана антивирусната заштита.
28	Антивирусната заштита треба да има можност за заштита на размената на електронска пошта од малициозен софтвер и спам,скенирање на интернет сообраќајот на минимум следниве протоколи: IMAP, SMTP, POP3, без разлика на тоа кој е-меил клиент се користи; без разлика на типот на протокол (вклучувајќи го минимум MAPI, HTTP) како дел од операцијата на плагини инкорпорирани во е-меил програмот на минимум Microsoft Office Outlook или еквивалентни.
29	Антивирусната заштита треба да има можност за бришење/преименување

	на одредени типови на датотеки, дефинирани од страна на администратор, во рамки на архиви.
30	Антивирусната заштита треба да има можност за заштита од програми за auto redial, блокирање на банери, поп-апи, малициозни сценарија симнувани од вебстрани и идентификација на страни за крадење на идентитет.
31	Антивирусната заштита треба да поддржува креирање на правила за контрола на пристапот до веб страни според преддефинирани категории на производителот, типови на содржини или експлицитно наведени URL-а. Можност за аплицирање на правилата по корисник/група од ActiveDirectory.
32	Антивирусната заштита треба да поддржува контрола за инсталација/стартување на програми која го регулира стартувањето на програми со правила со критериуми: патека до фолдерот со егзекутабилнатадатотека на програмата, егзекутабилнатадатотека на програмата на тврдиот диск, верзијата, името и издавачот на програмата, сертификатот на дигиталниот потпис на програмата, и MD5/SHA-256 хеш на егзекутабилнатадатотека на програмата.
33	Антивирусната заштита треба да поддржува генерирање на извештаи за блокирани извршувања на програми во тестен мод на работа.
34	Антивирусната заштита треба да поддржува контрола на преземањето на DLL модули и драјвери.
35	Антивирусната заштита треба да има можност за контрола на извршувањето на скрипти и DLL модули.
36	Антивирусната заштита треба да има можност за контрола на извршување на скрипти во PowerShell интерпретер.
37	Антивирусната заштита треба да има можност за поставување на Default Deny полиса со блокирање на извршувањето на сите програми освен оние експлицитно дозволени од администраторот.
38	Антивирусната заштита треба да има можност за користење на преддефинирани категории на апликации од страна на производителот на антивирусната заштита при креирање на правилата за блокирање на програми.
39	Антивирусната заштита треба да има можност за дефинирање на два модови на работа на инсталираните програми: whitelist и blacklist.
40	Антивирусната заштита треба да има можност да ги разликува датотеките по минимум следните технологии: Signature базирани анализи, Heuristic базирани анализи, iSwift и ichecker базирано скенирање.
41	Антивирусната заштита треба да поддржува "roll back" опции при операциите на дезинфекција (под "roll back" се подразбира враќање на поставувањата и промените кои се направени на датотечниот систем и

	регистрите).
42	Антивирусната заштита треба да поддржува "Bring Your Own Device (BYOD)" иницијатива и треба да вклучува "containerization" опции со цел да се осигура дека компаниските и личните податоци се чуваат во различни контејнери на корисничките уреди.
43	Антивирусната заштита треба да има една инсталацискадатотека со централизирана конфигурација и менаџмент на полисите со заеднички дистрибуциски механизам во комбинација на "push" и "pull" технологија за штедливо искористување на мрежните ресурси.
44	Решението треба да вклучува и алатки за далечинска дијагноза и инсталација кои ќе му помогнат на администраторот побрзо и поефикасно да ги отстрани можните проблеми.
45	Антивирусната заштита треба да има можност за поставување грануларен извештај и ad-hoc извештај.
46	Антивирусната заштита треба да има можност за поставување на управувачка конзола на оддалечено место и преку ваква управувачка конзола на оддалеченото место да се управува со персоналните компјутери во оддалеченото место. На овој начин ќе се штедат мрежните ресурси.
47	За активности поврзани со автоматско ажурирање/апдејтување на дефинициите на антивирусната заштита, истата треба да нуди можност за избор помеѓутри или повеќе извори од кои ќе се врши ажурирање/апдејтување, меѓу кои треба да има барем двеоддалечени места и барем едно локалноместо.
48	Антивирусната заштита треба да овозможува управување со процесот на инсталација на програмата за антивирусната заштитанаперсоналните компјутери како иавтоматско ажурирање/апдејтување преку централно/дистрибуирано складиште и веб сајт.
49	Антивирусната заштита треба да има можност за скенирање на ранливости и потребни ажурирања/апдејтувања во персоналните компјутери преку вградена компонента за скенирање.
50	Антивирусната заштита треба да има можност за преглед на пронајдени ранливости и препорачани акции за нивно отстранување.
51	Антивирусната заштита треба да поддржува хиерархиски директориум на политики за секој продукт и категорија на поставувања на персоналните компјутери, можност за креирање, измена, бришење и снимање/вчитување на политики. Политиките треба да се наследуваат од погорните кон подолните хиерархиски нивоа на директориумот на објекти.
52	Антивирусната заштита треба да има индикатор за нивото на заштита на системите при вршење измени на политиките. Можност за приказ на

	нотификација при оневозможување на клучни компоненти од антивирусната заштита.
53	Антивирусната заштита треба да има можност за креирање на политики за управување со секој аспект на антивирусната заштита.
54	Антивирусната заштита треба да има можност за синхронизација со Active Directory, целосно или делумно (специфични CN/OU) или директно користење на Active Directory на компјутерски сметки.
55	Антивирусната заштита треба да има можност за команди за (де)инсталација/„будење“ на клиенти, преглед на настани, доделување/модифицирање на политики, доделување/модифицирање/бришење на ознаки.
56	Антивирусната заштита треба да има можност за автоматско инсталирање на новите компјутери во ActiveDirectory ("auto-discovery").
57	Антивирусната заштита треба да има можност за автоматизација на работни задачи: синхронизација, креирање на циклични извештаи и нивно праќање по електронска пошта во интервал по избор.
58	Антивирусната заштита треба да има можност за избор на типот на настаните кои се испраќаат по електронска пошта.
59	Антивирусната заштита треба да има можност за доделување на грануларни привилегии на корисници од ActiveDirectory за работа на централната управувачка конзола. Треба да постојат најмалку: администратори со целосен пристап, администратори со делумен пристап и ревизори со пристап за читање.
60	Антивирусната заштита треба да има можност за водење на централна евиденција на настани со алатки за пребарување (филтрирање).
61	Антивирусната заштита треба да има можност за избор од готови извештаи за бројот на инсталации со тековни верзии на антивирусната заштита, антивирусните дефиниции и број на откриени закани.
62	Антивирусната заштита треба да има можност за креирање на ad-hoc извештаи со графички кориснички интерфејс со опции за измена, бришење, преглед на команда, снимање/вчитување и стартување.
63	Антивирусната заштита треба да има можност за креирање на извештај за настани на персоналните компјутери, со опции за филтрирање по време, IP адреса, идентификација на настан, опис на настан, категорија на настан, идентификација на персонален компјутер, акција, верзија итн., со команди за креирање исклучоци, прикажување на систем.
64	Антивирусната заштита на сервери треба да нуди можност за мониторирање на споделените фолдери на серверот со анализирање на однесувањето на процеси за поврзаност со криптовируси (ransomware).
65	Решението за заштита на сервери треба да нуди можност за блокирање на хостови кои се обидуваат да извршат малициозна активност врз

	споделените фолдери според претходно анализирање на однесувањето. Можност за регулирање на временскиот интервал во кој хостовите ќе бидат блокирани.

Функционалности на анти-спам заштита на системот за размена на електронска поштаза Microsoft Exchange Server (верзии 2013, 2016, 2019).

Ред. Бр.	Барања за анти-спам заштита на системот за размена на електронска пошта:
1	Анти-спам заштита на системот за размена на електронска пошта треба да може да се интегрира со Mail Transfer Agent (MTA) за да се овозможи функционалност на засебен gateway/relay.
2	Анти-спам заштита на системот за размена на електронска пошта треба да може да се интегрира со Microsoft Active Directory, LDAP или еквивалентно со можност за енкриптирана комуникација до овие сервери со TLS/SSL.
3	Анти-спам заштита на системот за размена на електронска пошта треба да може да го скенира влезниот и излезниот сообраќај и електронската пошта (вклучително "Public Folder-ите") што се наоѓаат восистемот за размена на електронска пошта, против "malware" закани.
4	Анти-спам заштита на системот за размена на електронска пошта треба да поддржува SNMP или еквивалентно.
5	Анти-спам заштита на системот за размена на електронска пошта треба да има веб базиран интерфејс за управување со самиот анти-спам систем.
6	Можност за интеграција со постоечко анти-вирусно решение со цел централизиран мониторинг.
7	Автоматско обновување на дефинициите - можност за избор на извори од кои ќе се врши обновувањето, и тоа од внатрешни/надворешни адреси и локални патеки.
8	Можност за ажурирање на верзијата на анти-спам заштитата на системот за размена на електронска пошта преку неговиот веб интерфејс.
9	Централен преглед (dashboard) со статистики за скенираната електронска пошта, најновите забележани безбедности закани, како и искористеноста на ресурси од страна на анти-спам заштита на системот за размена на електронска пошта.
10	Треба да има пристап до интерфејсот на анти-спам заштита на системот за размена на електронска поштазаснован на улоги. анти-спам заштита на системот за размена на електронска пошта Анти-спам заштита на системот за размена на електронска пошта треба да има можност за креирање на посебни профили за Administrator и Helpdesk со различни привилегии.
11	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за управување со редовите на чекање во системот за размена на електронска пошта.

12	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за пребарување и манипулација со пораките во редовите на чекање во системот за размена на електронска пошта според тип на ред на чекање, ID на електронската порака, име на испраќач/примач на електронска порака, период во кој е испратена/примена електронската порака и големина на електронската порака.
13	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за конфигурација на повеќе домени од кои ќе се прифаќа електронска пошта.
14	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за обработка на 10 електронски пораки во секунда со просечна големина од 50KB при default поставувања на системот, иможност за зголемување на системот во зависност од потребите.
15	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за скенирање на појдовните/дојдовнитеелектронски пораки за сите типови на закани (spam, phishing, malware, итн.).
16	Анти-спам заштита на системот за размена на електронска пошта треба да има еуристика при скенирањето иможност за регулирање на нивото на еуристика која се употребува.
17	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за регулирање на времето за скенирање на електронските пораки како и можност за регулирање на нивото на скенирање на вгнездувањата во додатоците прикачени во електронските пораки.
18	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за TLS тунелирање помеѓу организации за безбеден пренос на електронска пошта со вклучена можност за управување со сертификатите.
19	Анти-спам заштита на системот за размена на електронска пошта треба да има поддршка за автентикациски технологии за пораките: SPF, DKIM, DMARC или еквивалентно.
20	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за филтрирање на електронската пошта која е означена како спам (unsolicited mail) пред таа да дојдат до електронските поштенски сандачињата.
21	Користење на облак технологија со за ажурирање/апдејтување во реално време со цел заштита од zero-hour спам и спам епидемии.
22	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за cloud-асистирано репутациско филтрирање -сместување на сомнителните пораки во карантин пред да се проверат со најновите дефиниции со цел заштита од непознат спам и лажно позитивни.
23	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за креирање на полиси за откривање и блокирање на

	непосакувана масовна електронска пошта.
24	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за Cloud-асистирано скенирање на појдовниата/дојдовниатаелектронска пошта за вируси во реално време.
25	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за заштита од zero day и таргетирани напади со користење на посебен модул за напредна заштита.
26	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за cloud-асистирано скенирање на URL адреси во електронските пораки иможност за блокирање на електронски пораки кои содржат URL адреси до малициозни веб страни.
27	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за cloud-асистирано скенирање на електронска пошта за phishing иможност за блокирање на електронска пошта која содржат URL адреси до phishing веб страни.
28	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за филтрирање на пораките врз основа на додатоците кои ги содржат според нивното име и/или според нивниот формат.
29	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за откривање, известување, означување, неутрализирање или сместување во карантин на инфицирани, сомнителни, оштетени датотеки, датотеки заштитени со лозинка или датотеки кај кои се случила грешка при скенирањето.
30	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за откривање на Reverse DNS check (anti-spoofing).
31	Анти-спам заштита на системот за размена на електронска пошта треба да има складиште за електронски пораки кои биле откриени како безбедносназакана од страна на анти-спам заштита (карантин).
32	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за одредување на големината на меморискиот простор кој го користи карантинот, со можност за известување кога овој меморискипростор е приближно пополнет.
33	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за одредување на акции во случај кога карантинот е недостапен.
34	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за пребарување и ослободување на пораки во карантинот според име на испраќач/примач, наслов на пораката, ID на пораката, период во кој е испратена/примена, големина на пораката како и правило кое било причина за поставување на електронската порака во карантин.
35	Анти-спам заштита на системот за размена на електронска пошта треба да

	има можност за ограничување на големината на појдовните/дојдовните електронски пораки.
36	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за користење на предефинирани whitelists/blacklists правила како и креирање на нови правила.
37	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за креирање правила по корисник, e-mail адреса или IP адреса, какои за група од корисници.
38	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за креирање на дневни, неделни, месечни или извештаи за период одреден од страна на корисникот, нивно извезување во PDF документ, преглед и манипулација со генерирани извештаи како иможност за нивно испраќање до одреден корисник или група на корисници.
39	Анти-спам заштита на системот за размена на електронска пошта треба да има можност за избор на настани за кои ќе бидат испраќани известувања, менување на содржината на електронските пораки кои се испраќаат како известување, како и избор на корисник или група од корисници до кои ќе се испраќаат известувањата.
40	Решението треба да има можност да се инсталира во виртуелна машина во VMware/Microsoft Hyper-V или еквивалентна виртуелна околина.

ОБВРСКИ НА ДОГОВОРНИОТ ОРГАН

Член 11

Договорниот орган е должен да ја плати договорената цена на носителот на набавката, по извршената услуга а во рок од 60 дена од денот на доставувањето на фактура од страна на носителот на набавката, пополнета на начин пропишан со тендерската документација.

Лице задолжено за реализација на договорот кај Договорниот орган е Танче Горгиевски или друго лице овластено од Министер.

ОБЕШТЕТУВАЊЕ

Член 12

Договорните страни се должни да ги исполнат обврските кои произлегуваат од овој Договор.

Член 13

Поради неисполнување на обврските од страна на носителот на набавката договорниот орган има право на надомест на обична штета и испуштена корист.

РЕШАВАЊЕ НА СПОРОВИ

Член 14

Сите евентуални спорови и недоразбирања кои би произлегле од овој Договор, договорните страни ќе ги решаваат во духот на добрите деловни обичаи со меѓусобно договарање.

Член 15

Доколку договорните страни не постигнат обострано прифатливо решение сите евентуални спорови ќе ги решава надлежниот суд во Скопје.

УСЛОВИ ЗА ПРЕКИНУВАЊЕ ИЛИ РАСКИНУВАЊЕ НА ДОГОВОРОТ

Член 16

Кога носителот на набавката не ќе ја исполни својата обврска, другата договорна страна, може да бара исполнување на обврските или да го раскине договорот, а во секој случај има право на надомест на штета и активирање на банкарска гаранција.

Член 17

Кога носителот на набавката не ќе ја исполни својата обврска во определениот рок, договорниот орган има право да му остави дополнителен рок за исполнување на обврската .

Дополнителниот рок може да се остави само во случај кога Договорниот орган не трпи штета и во тој случај нема да се бара надомест на штета и да се активира банкарска гаранција .

Член 18

Ако носителот на набавката не ја исполнил својата обврска во определениот рок, не ја исполни обврската ни во дополнителниот рок, Договорниот орган може да го раскине договорот.

Во случај на раскинување на договорот поради неисполнување на оврските во определениот рок и во дополнителниот рок, Договорниот орган има право на надомест на штета и право да ја активира банкарската гаранција.

КОРУПЦИСКО ИЛИ ИЗМАМНИЧКО ОДНЕСУВАЊЕ

Член 19

Договорните страни се согласни да ги применат највисоките стандарди за етичко и законито однесување за време на реализација на овој Договор.

ЗАВРШНИ И ОПШТИ ОДРЕДБИ

Член 20

Договорот за јавна набавка во текот на неговата важност може да се дополни и/или измени само врз основа на член 119 од Законот за јавни набавки .

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

Одредбите од овој договор можат да се изменат и/или дополнат со склучување на Договорот за изменување и дополнување на основниот Договор.

Дополнувањата и измените на овој договор се важечки ако се направени во писмена форма и ако се потпишани од двете договорни страни.

Член 21

Ниту една договорна страна нема право своите обврски да ги пренесе на трета страна, без взаемна писмена согласност.

Член 22

Овој Договор е составен во 4 (четири) примероци, од кои секоја страна задржува по 2 (два) примерока и стапува во сила со денот на неговото склучување.

МИНИСТЕР
Јованка Тренчевска

Договорен орган

Овластено лице,
Стевчо Ристески

Носител на набавката

Друштво за комуникациски услуги
А1 Македонија ДООЕЛ Скопје
30

Изготвил:Маја Додевска Пешевска
Согласен: Славица Костовска
Контролирал: Љубица Панова