Digitalni podpis

Podpisnik: Urška Kos
Izdajatelj: SIGOV-CA
Številka certifikata: 22FA2029000000005
Potek veljavnosti: 29. 10. 2030
Čas podpisa: 13. 11. 2026 11:54
Št. dok.: 430-86/2026-9

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA FINANCE
UPRAVA REPUBLIKE SLOVENIJE ZA JAVNA PLAČILA

Dunajska cesta 48, p. p. 3543, 1001 Ljubljana

T: 01 475 16 51
E: ujp@ujp.gov.si
www.ujp.gov.si

Številka: 430-86/2026-9
Datum: 13. 11. 2026

DOKUMENTACIJA

ZA ODDAJO JAVNEGA NAROČILA

Predmet javnega naročila:

dobava, namestitev, konfiguracija in garancijsko vzdrževanje dveh (2) kompletov požarnih pregrad v komunikacijskem omrežju

Vrsta postopka:
postopek naročila male vrednosti (47. člen ZJN-3)

Oznaka javnega naročila:
4/2026-JNMV-PP

KAZALO:

I. POVABILO K ODDAJI PONUDBE ... 3
1. NAROČNIK ... 3
2. PREDMET JAVNEGA NAROČILA ... 3
3. NAČIN ODDAJE JAVNEGA NAROČILA ... 3
4. KRAJ OPRAVLJANJA STORITEV ... 3
5. TRAJANJE JAVNEGA NAROČILA ... 3
6. ROK IN NAČIN PREDLOŽITVE PONUDB ... 3
7. ČAS IN NAČIN ODPIRANJA PONUDB ... 4
8. PRAVNA PODLAGA ... 4
9. RAZPISNA DOKUMENTACIJA, OBVESTILA IN POJASNILA ... 5
9.1. Prevzem razpisne dokumentacije ... 5
9.2. Sprememba in dopolnitev razpisne dokumentacije ... 5
9.3. Dodatna pojasnila in obvestila ... 5
10. SPLOŠNE ZAHTEVE ZA PRIZNANJE SPOSOBNOSTI IN SODELOVANJE V POSTOPKU ... 5
10.1. Samostojna ponudba, pri kateri ne sodelujejo drugi gospodarski subjekti ... 5
10.2. Ponudba, pri kateri sodelujejo drugi gospodarski subjekti ... 6
10.2.1. Splošne zahteve ... 6
10.2.2. Skupna ponudba ponudnikov ... 7
10.2.3. Ponudba s podizvajalci ... 8
10.2.4. Ponudba z uporabo zmogljivosti gospodarskih subjektov iz 81. člena ZJN-3 ... 9
10.2.5. Ponudba, pri kateri sodeluje tuja pravna ali fizična oseba ... 9
11. POGOJI ZA PRIZNANJE SPOSOBNOSTI IN DOKAZILA ... 10
12. MERILO ZA OCENJEVANJE PONUDB IN IZBIRO PONUDNIKA ... 16
13. DRUGA DOLOČILA ZA PRIPRAVO PONUDBE ... 16
13.1. Ponudbena dokumentacija ... 16
13.2. Obrazec ESPD za vse gospodarske subjekte ... 17
13.3. Obrazec »Ponudba / Predračun« ... 17
13.4. Obrazec 3 »Izjava o tehnični in funkcionalni skladnosti opreme in storitev« ... 19
13.5. Obrazec 4 »Izjava o tehnični in strokovni sposobnosti« ... 19
13.6. Obrazec 5 »Referenčno potrdilo« ... 19
13.7. Ostale priloge ... 19
13.8. Jezik, v katerem mora ponudnik pripraviti ponudbo ... 19
13.9. Obseg ponudbe ... 19
13.10. Rok veljavnosti ponudbe ... 19
13.11. Stroški ponudbe ... 20
13.12. Označitev zaupnih podatkov ... 20
13.13. Sprememba ali dopolnitev ponudbe ... 20
13.14. Protikorupcijska določba ... 20
14. DAJANJE NERESNIČNIH ALI ZAVAJAJOČIH IZJAV IN DOKAZIL ... 20
15. USTAVITEV POSTOPKA IN ODSTOP OD IZVEDBE JAVNEGA NAROČILA ... 21
16. OBVESTILO O ODLOČITVI O ODDAJI NAROČILA ... 21
17. POGODBA ... 21
18. VARSTVO OSEBNIH PODATKOV ... 22
19. PRAVNO VARSTVO ... 22
II. PREDMET JAVNEGA NAROČILA IN TEHNIČNE ZAHTEVE ... 24
1. Opis trenutnega komunikacijskega omrežja ... 24
2. Predmet javnega naročila ... 24
2.1. Splošne zahteve ... 24
2.2. Tehnične zahteve in lastnosti obeh požarnih pregrad ... 24
2.3. Lokacija in obseg izvajanja storitev ... 29
2.4. Rok za dobavo in namestitev opreme ... 30
2.5. Garancijski pogoji ... 30
2.6. Režim garancijskega vzdrževanja opreme ... 30
3. Vzorec pogodbe ... 32
III. PONUDBENA DOKUMENTACIJA ... 68
Obrazec 2 – Ponudba / Predračun ... 68
Obrazec 3 – Izjava o tehnični in funkcionalni skladnosti ponujene opreme in storitev ... 70
Obrazec 4 – Izjava o tehnični in strokovni sposobnosti ... 77
Obrazec 5 – Referenčno potrdilo ... 78
Obrazec 6 – Izjava tuje fizične osebe o nekaznovanosti ... 79

I. POVABILO K ODDAJI PONUDBE

1. NAROČNIK

Naročnik je Republika Slovenija, Ministrstvo za finance, **Uprava Republike Slovenije za javna plačila**, Dunajska cesta 48, p. p. 3543,1001 Ljubljana, matična številka 1572814000, davčna številka 10641424, šifra proračunskega uporabnika 16187 (v nadaljnjem besedilu: naročnik ali UJP).

Naročnik vabi vse zainteresirane ponudnike, da predložijo ponudbe na priloženih obrazcih, skladno z zahtevami iz razpisne dokumentacije.

2. PREDMET JAVNEGA NAROČILA

Predmet javnega naročila je dobava, namestitev, konfiguracija in garancijsko vzdrževanje dveh (2) kompletov požarnih pregrad v komunikacijskem omrežju po specifikaciji, zahtevah in pogojih, ki so podrobneje opredeljeni v II. poglavju te razpisne dokumentacije *(»II. Predmet javnega naročila in tehnične zahteve«).*

3. NAČIN ODDAJE JAVNEGA NAROČILA

Javno naročilo se oddaja po postopku naročila male vrednosti v skladu s 47. členom Zakona o javnem naročanju Uradni list RS, št. 91/15, 14/18, 121/21, 10/22, 74/22 – odl. US, 100/22 – ZNUZSZS, 28/23, 88/23 – ZOPNN-F in 83/25 - ZOUL; v nadaljnjem besedilu: ZJN-3).

4. KRAJ OPRAVLJANJA STORITEV

Storitve, ki so predmet tega javnega naročila, se bodo izvajala na lokacijah naročnika v Ljubljani in v Kopru ter na lokacijah ponudnika, ki bo izbran v tem postopku, oziroma na daljavo (po telekomunikacijski ali elektronski poti prek spleta).

5. TRAJANJE JAVNEGA NAROČILA

Rok za dobavo, namestitev in konfiguracijo ter primopredajo obeh požarnih pregrad (vključno s tehnično dokumentacijo) in izvedbo vseh storitev, ki so predmet javnega naročila, je 90 dni od dneva podpisa pogodbe.

Garancijsko vzdrževanje se izvaja 36 mesecev od primopredaje obeh požarnih pregrad in pripadajoče tehnične dokumentacije.

6. ROK IN NAČIN PREDLOŽITVE PONUDB

Ponudniki morajo ponudbe predložiti v elektronski obliki v informacijski sistem e-JN (v nadaljnjem besedilu: sistem e-JN) na spletnem naslovu https://ejn.gov.si oziroma Ponudnik (gov.si) v skladu z dokumentom *»Navodila za uporabo informacijskega sistema e-JN: PONUDNIKI«* (v nadaljnjem besedilu: Navodila za uporabo e-JN), ki je dostopno na navedenem spletnem naslovu in zavihku Več informacij ponudniki (gov.si).

Ponudniki se morajo pred oddajo ponudbe registrirati na spletnem naslovu, navedenem v prejšnjem odstavku, skladno z Navodili za uporabo e-JN. Če je ponudnik že registriran v sisteme e-JN, se v aplikacijo prijavi na istem naslovu.

Uporabnik ponudnika, ki je v sistemu e-JN pooblaščen za oddajanje ponudb, ponudbo odda s klikom na gumb »Oddaj«. Sistem e-JN ob oddaji ponudbe zabeleži identiteto uporabnika in čas oddaje ponudbe. Uporabnik z dejanjem oddaje ponudbe izkaže in izjavi voljo v imenu gospodarskega subjekta oddati zavezujočo ponudbo (18. člen Obligacijskega zakonika[1]). Z oddajo ponudbe je ta zavezujoča za čas, naveden v ponudbi, razen če jo uporabnik ponudnika umakne ali spremeni pred potekom roka za oddajo ponudb.

Ponudba se šteje za pravočasno oddano, če jo naročnik prejme v sistemu e-JN **do 3. 12. 2026 do 12.00 ure**. Za oddano ponudbo se šteje ponudba, ki je v sistemu e-JN označena s statusom »ODDANA«.

Ponudnik lahko do roka za oddajo ponudb svojo ponudbo umakne ali spremeni. Če ponudnik v sistemu e-JN svojo ponudbo umakne, se šteje, da ponudba ni bila oddana in je naročnik v sistemu e-JN tudi ne bo videl. Če ponudnik svojo ponudbo v sistemu e-JN spremeni, je naročniku v tem sistemu odprta zadnja oddana ponudba.

Po preteku roka za predložitev ponudb ponudbe ne bo več mogoče oddati.

Dostop do povezave za oddajo elektronske ponudbe v tem postopku javnega naročila je objavljen na portalu javnih naročil oziroma v spletnem obrazcu, ki se nanaša na predmetno javno naročilo.

Vse ponudbe, oddane v fizični (papirni) obliki oziroma izven sistema e-JN, bo naročnik izločil iz postopka odpiranja ponudb in jih neodprte vrnil ponudnikom. Če na ovojnici ne bo ponudnikovega naslova, bo naročnik po pravnomočnosti odločitve o oddaji javnega naročila zaprto ovojnico komisijsko uničil.

7. ČAS IN NAČIN ODPIRANJA PONUDB

Odpiranje ponudb bo potekalo avtomatično v sistemu e-JN dne **3. 12. 2026** in se bo začelo **ob 13:00 uri** na spletnem naslovu https://ejn.gov.si.

Odpiranje poteka tako, da sistem e-JN samodejno ob uri, ki je določena za javno odpiranje ponudb, prikaže podatke o ponudniku, skupni ponudbeni vrednosti ponudbe ter omogoči dostop do dokumenta, ki ga ponudnik naloži v sistem e-JN pod razdelek »Skupna ponudbena cena«, v del »Predračun«. Ponudniki, ki so oddali ponudbe, imajo te podatke v informacijskem sistemu e-JN na razpolago v razdelku »Zapisnik o odpiranju ponudb«.

8. PRAVNA PODLAGA

Naročnik izvaja postopek oddaje javnega naročila na podlagi veljavnega ZJN-3 in podzakonskih predpisov, ki urejajo javno naročanje in so dostopni v sistemu e-JN Veljavni predpisi (gov.si).

Poleg predpisov iz prejšnjega odstavka se javno naročilo oddaja in po sklenitvi pogodbe izvaja v skladu z veljavnimi predpisi in akti, navedenimi v tej razpisni dokumentaciji oziroma v vzorcu pogodbe.

[1] Obligacijski zakonik (Uradni list RS, št. 97/07 – uradno prečiščeno besedilo, 64/16 – odl. US in 20/18 – OROZ631)

9. RAZPISNA DOKUMENTACIJA, OBVESTILA IN POJASNILA

9.1. Prevzem razpisne dokumentacije

Razpisno dokumentacijo lahko ponudniki prevzamejo na portalu javnih naročil v okviru obvestila o naročilu, ki se nanaša na predmetno javno naročilo.

9.2. Sprememba in dopolnitev razpisne dokumentacije

Naročnik si pridržuje pravico, da v skladu s 67. členom ZJN-3 spremeni ali dopolni razpisno dokumentacijo, ter da v primeru bistvenih sprememb ali dopolnitev razpisne dokumentacije podaljša rok za oddajo ponudb tako, da omogoči ponudnikom ustrezen čas za upoštevanje dopolnitev pri pripravi ponudb. Vsaka sprememba ali dopolnitev postane sestavni del razpisne dokumentacije in bo objavljena na portalu javnih naročil.

9.3. Dodatna pojasnila in obvestila

Komunikacija s ponudniki o vprašanjih v zvezi s predmetom in obsegom naročila ter pripravo ponudbe poteka izključno na portalu javnih naročil.

Naročnik bo kot pravočasno zahtevo za pojasnilo razpisne dokumentacije oziroma kakršnokoli drugo vprašanje v zvezi z naročilom štel kot pravočasno, v kolikor bo prek portala javnih naročil poslano najpozneje do vključno **30. 11. 2026 do 10.00 ure**.

Na zahteve za pojasnila oziroma druga vprašanja v zvezi z naročilom, zastavljena po tem roku, naročnik ne bo odgovarjal.

Vsi odgovori na vprašanja ponudnikov, objavljeni na portalu javnih naročil, postanejo sestavni del razpisne dokumentacije in so za ponudnike in naročnika obvezujoči.

10. SPLOŠNE ZAHTEVE ZA PRIZNANJE SPOSOBNOSTI IN SODELOVANJE V POSTOPKU

10.1. Samostojna ponudba, pri kateri ne sodelujejo drugi gospodarski subjekti

Ponudnik mora izpolnjevati vse pogoje na dan, ko se izteče rok za oddajo ponudb, razen če je v tej razpisni dokumentaciji določeno drugače.

Za dokazovanje izpolnjevanja pogojev mora ponudnik priložiti dokazila, kot so navedena za vsakim zahtevanim pogojem.

Ob predložitvi ponudbe gospodarski subjekt predloži »Enotni evropski dokument v zvezi z oddajo javnega naročila – ESPD« (v nadaljnjem besedilu: obrazec ESPD), ki vključuje posodobljeno lastno izjavo, kot predhodni dokaz v zvezi z izpolnjevanjem pogojev. Obrazec ESPD predstavlja uradno izjavo gospodarskega subjekta, da ne obstajajo razlogi za izključitev in da izpolnjuje pogoje za sodelovanje, hkrati pa zagotavlja ustrezne informacije, ki jih zahteva naročnik. V obrazcu ESPD je naveden tudi uradni organ ali tretja oseba, odgovorna za izdajo dokazil, vključuje pa tudi uradno izjavo o tem, da bo gospodarski subjekt na zahtevo in brez odlašanja sposoben predložiti ta dokazila.

Navedbe v obrazcu ESPD in/ali dokazila, ki ji predloži gospodarski subjekt, morajo biti veljavni.

Gospodarski subjekt mora v obrazcu ESPD navesti vse informacije, na podlagi katerih bo naročnik potrdila ali druge informacije pridobil v nacionalni bazi podatkov, ter v predmetnem obrazcu podati soglasje, da dokazila pridobi naročnik.

Naročnik lahko kadarkoli med postopkom ponudnike povabi, da predložijo vsa dokazila ali del dokazil v zvezi z navedbami v obrazcu ESPD, ter da po potrebi dopolnijo ali pojasnijo predložena dokazila (potrdila, izjave), ki dokazujejo izpolnjevanje pogojev, razen dokazil, ki se vodijo v uradnih evidencah državnih organov, organov lokalnih skupnosti ali nosilcev javnih pooblastil na območju Republike Slovenije. Če pozvani ponudnik v roku, ki ga določi naročnik, naročniku ne posreduje zahtevanih dokazil, bo naročnik njegovo ponudbo izključil.

Ponudnik lahko dokazila o neobstoju izključitvenih razlogov in izpolnjevanju pogojev za sodelovanje predloži tudi sam. Naročnik si pridržuje pravico do preveritve verodostojnosti predloženih dokazil.

Naročnik si pridržuje pravico, da pred oddajo javnega naročila od ponudnika, kateremu se je odločil oddati javno naročilo, zahteva, da predloži najnovejša dokazila (potrdila, izjave) kot dokaz neobstoja razlogov za izključitev, določenih v razpisni dokumentaciji.

Če ni v tej razpisni dokumentaciji za posamezne dokumente drugače določeno, zadošča predložitev kopij zahtevanih dokumentov. Naročnik si pridržuje pravico do vpogleda v izvirne dokumente. V primeru, da bo naročnik naknadno zahteval izvirne dokumente, jih mora ponudnik v roku petih (5) dni po prejemu poziva predložiti na vpogled.

Obrazci izjav, ki jih mora predložiti ponudnik v ponudbi, so del razpisne dokumentacije. Izjave so lahko predložene na teh obrazcih ali na ponudnikovih, ki pa vsebinsko bistveno ne smejo odstopati od obrazcev iz razpisne dokumentacije. Obrazci in izjave ter ostali dokumenti ponudnika morajo biti podpisani s strani osebe, ki ima pravico zastopanja ponudnika. V primeru, da obrazec/izjavo podpiše pooblaščena oseba, ki ni zakoniti zastopnik, mora biti k ponudbi priloženo pooblastilo zakonitega zastopnika osebi, ki je pooblaščena za podpis dokumentacije.

Obrazci, izjave, potrdila in drugi dokumenti so lahko podpisani z elektronskim ali lastnoročnim podpisom. Uporaba žiga na navedenih dokumentih ni obvezna.

Če obstaja naročnikova zahteva, koliko stari so lahko dokumenti, ki jih ponudnik prilaga kot dokazila, je to navedeno ob vsakem posameznem dokazilu. Če ni navedeno ničesar, starost dokumenta ni pomembna, odražati pa mora zadnje stanje. Dokumenti morajo ne glede na določeno oziroma zahtevano največjo dopuščeno starost vedno odražati zadnje stanje. Začetek roka za starost dokumentov se šteje od dneva objave obvestila o naročilu na portalu javnih naročil, razen če je pri posameznem dokazilu določeno drugače.

10.2. Ponudba, pri kateri sodelujejo drugi gospodarski subjekti

10.2.1. Splošne zahteve

Ponudnik lahko izpolnjuje pogoje za sodelovanje skupaj z drugimi ponudniki (partnerji skupne ponudbe) ali s podizvajalci ali tako, da se sklicuje na zmogljivosti drugih gospodarskih subjektov, pod pogojem, da bo podizvajalec oziroma gospodarski subjekt izvedel posel v delu, v katerem se ponudnik sklicuje na njegove kapacitete in bodo le-te izkoriščene oziroma uporabljene pri izvedbi predmetnega naročila. V tem primeru mora ponudnik v ponudbi predložiti njihove dokumente, ki se nanašajo na dokazovanje pogojev, in v primeru sklicevanja na kapacitete drugih subjektov dokazilo, da bo zaradi tega imel na voljo sredstva za izvedbo naročila, in sicer pisni dogovor z drugim subjektom, sklenjenim za ta namen.

Pogoje za priznanje sposobnosti morajo izpolnjevati tudi gospodarski subjekti na kapacitete katerih se sklicuje ponudnik, skladno z 81. členom ZJN-3.

Za ponudbe, pri katerih sodelujejo drugi gospodarski subjekti, je potrebno upoštevati še zahteve, ki so opredeljene v naslednjih točkah te razpisne dokumentacije:

- 10.2.2 *(Skupna ponudba ponudnikov),*
- 10.2.3 *(Ponudba s podizvajalci),*
- 10.2.4 *(Ponudba z uporabo zmogljivosti drugih gospodarskih subjektov iz 81. člena ZJN-3),*
- 10.2.5. *(Ponudba, pri kateri sodeluje tuja pravna ali fizična oseba)*.

Ponudnik lahko samostojno ali v skupni ponudbi nastopa le v eni ponudbi. Gospodarski subjekt je lahko podizvajalec pri različnih ponudnikih oziroma ponudbah pod pogojem, da v tem postopku ni oddal samostojne ponudbe ali da ne sodeluje kot partner skupne ponudbe. Če bo posamezni gospodarski subjekt nastopal v več kot eni ponudbi (hkrati samostojno in v okviru skupne ponudbe ali kombinaciji teh ter hkrati kot podizvajalec v drugi ponudbi), bo naročnik izločil vse ponudbe, pri katerih sodeluje gospodarski subjekt, ki krši to prepoved.

10.2.2. Skupna ponudba ponudnikov

V primeru, da skupina ponudnikov predloži skupno ponudbo, mora vsak ponudnik izpolnjevati vse pogoje iz te razpisne dokumentacije, razen če je pri posameznem pogoju določeno, da se lahko izpolni kumulativno. Kumulativno izpolnjevanje pogoja pomeni, da celotne zahteve obravnavanega pogoja lahko skupaj izpolnijo vsi gospodarski subjekti, ki nastopajo v ponudbi.

Vsi ponudniki v skupni ponudbi morajo izpolniti obrazec ESPD posamično in v njem navesti vse zahtevane podatke.

V primeru, da skupina ponudnikov predloži skupno ponudbo, bo naročnik iz postopka javnega naročanja izločil skupno ponudbo, če se izkaže, da je katerikoli izmed skupnih ponudnikov pred ali med postopkom javnega naročanja glede na storjena ali neizvedena dejanja v enem izmed položajev, ki so razlog za izključitev, razen če bo gospodarski subjekt uporabil možnost popravnih mehanizmov na način in pod pogoji, določenimi v ZJN-3 in tej razpisni dokumentaciji.
Naročnik si pridržuje pravico, da naknadno zahteva predložitev akta o skupni izvedbi naročila (npr. pogodbo ali sporazum o sodelovanju), v katerem bodo natančno opredeljene naloge in odgovornosti posameznih gospodarskih subjektov za izvedbo naročila zlasti naslednja vprašanja oziroma razmerja:

- podatki o sodelujočih partnerjih;
- imenovanje poslovodečega izvajalca pri izvedbi javnega naročila;
- pooblastilo poslovodečemu partnerju oziroma odgovorni osebi za zastopanje v odnosih z naročnikom, za sestavo, usklajevanje, podpis in predložitev ponudbe ter podpis pogodbe in ostala potrebna dejanja v zvezi s ponudbo in izvedbo javnega naročila;
- natančno opredeljene naloge oziroma storitve ter odgovornosti vsakega sodelujočega izvajalca v okviru izvedbe javnega naročila (področje dela oziroma specifikacija in vrednost blaga in storitev, ki jih bo dobavil/izvedel vsak partner v skupini, delež vsakega partnerja v skupini, kadri);
- izjava izvajalcev, da je imel poslovodeči partner v obdobju enega leta pred oddajo ponudbe ves čas pravočasno in v celoti poravnane svoje zapadle obveznosti do njih;
- izjava, da so vsi sodelujoči izvajalci seznanjeni z razpisno dokumentacijo, razpisnimi pogoji, merili za dodelitev javnega naročila, plačilnimi pogoji in pogodbenimi obveznostmi in da z njimi v celoti soglašajo;
- navedba, da vsi sodelujoči izvajalci odgovarjajo naročniku neomejeno solidarno za izvedbo javnega naročila in pogodbene obveznosti;
- način obračunavanja in plačila storitev (prek poslovodečega partnerja v skupini);
- določbe v primeru izstopa kateregakoli od partnerjev v skupini;

- reševanje sporov med partnerji v skupini;
- druge morebitne pravice in obveznosti med partnerji v skupini.

Ne glede na prejšnji odstavek ponudniki odgovarjajo naročniku solidarno.

10.2.3. Ponudba s podizvajalci

V primeru, da bo ponudnik pri izvedbi naročila sodeloval s podizvajalci, mora v obrazcu ESPD navesti vse podizvajalce ter vsak del javnega naročila, ki ga namerava oddati v podizvajanje. Ponudnik mora v ponudbi predložiti tudi izpolnjene in podpisane obrazce ESPD za vsakega podizvajalca, s katerim bo sodeloval pri naročilu, ter druga zahtevana dokazila o izpolnjevanju pogojev oziroma sposobnosti posameznega podizvajalca.

Pogoji, ki jih mora izpolnjevati podizvajalec, so podrobneje obrazloženi z dodatnimi pojasnili k posameznim pogojem ali v navodilih, ki so sestavni del posameznega obrazca iz te razpisne dokumentacije.

Če bodo pri podizvajalcu obstajali razlogi za izključitev oziroma ne bo izpolnjeval ustreznih pogojev za sodelovanje iz te razpisne dokumentacije, bo naročnik podizvajalca zavrnil in zahteval njegovo zamenjavo. Če ponudnik ne zagotovi drugega ustreznega podizvajalca v roku, ki ga določi naročnik, se ponudba zavrne oziroma izloči iz postopka.

Ponudnik mora za posameznega podizvajalca priložiti enaka dokazila za izpolnjevanje pogojev, določenih v prejšnjem stavku, kot jih mora priložiti zase, razen pri pogojih, kjer so že predvidena dokazila, ki jih mora predložiti podizvajalec.

Podizvajalci, navedeni v osnovni ponudbi, morajo izpolnjevati pogoje na dan oddaje ponudbe. V primeru vključitve novih podizvajalcev (npr. med izvajanjem pogodbe), se izpolnjevanje pogojev oziroma sposobnost podizvajalcev ugotavlja (ocenjuje) po stanju na dan, ko naročnik prejme obvestilo izbranega ponudnika o vključitvi novega podizvajalca.

V primeru oddaje javnega naročila in sklenitve pogodbe bo moral izbrani ponudnik med izvajanjem javnega naročila oziroma pogodbe naročnika obvestiti o morebitnih spremembah informacij, ki se nanašajo na podizvajalce, in poslati informacije o novih podizvajalcih, ki jih namerava naknadno vključiti v izvajanje pogodbe, in sicer najkasneje v petih dneh po spremembi. V primeru vključitve novih podizvajalcev bo moral glavni izvajalec skupaj z obvestilom posredovati tudi podatke in dokumente iz druge, tretje in četrte alineje drugega odstavka 94. člena ZJN-3.

Naročnik bo zavrnil vsakega naknadno nominiranega podizvajalca:
- če zanj obstajajo razlogi za izključitev, kot so navedeni v tej razpisni dokumentaciji ter zahteval zamenjavo,
- če bi to lahko vplivalo na nemoteno izvajanje ali dokončanje del,
- če novi podizvajalec ne izpolnjuje pogojev v zvezi z oddajo javnega naročila.

Neposredna plačila podizvajalcem, skladno z določbami 94. člena ZJN-3 in Uredbe o neposrednih plačilih podizvajalcu pri nastopanju ponudnika s podizvajalcem pri javnem naročanju (Uradni list RS, št. 66/07, 19/10 – ZJN-2B in 19/10 – ZJNVETPS-B), so obvezna le v primeru, če podizvajalec na način, določen v drugem in tretjem odstavku 94. člena ZJN-3, zahteva neposredna plačila, v nasprotnem primeru se upošteva šesti odstavek 94. člena ZJN-3. Le če podizvajalec zahteva neposredno plačilo, se šteje, da je neposredno plačilo podizvajalcu obvezno in obveznost zavezuje tako naročnika kot tudi glavnega izvajalca.

Kadar namerava ponudnik izvesti javno naročilo s podizvajalcem, ki zahteva neposredno plačilo v skladu z navedenim členom, mora:

- glavni izvajalec v pogodbi pooblastiti naročnika, da na podlagi potrjenega računa oziroma situacije s strani glavnega izvajalca neposredno plačuje podizvajalcu,
- podizvajalec predložiti soglasje, na podlagi katerega naročnik namesto ponudnika poravna podizvajalčevo terjatev do ponudnika,
- glavni izvajalec svojemu računu ali situaciji priložiti račun ali situacijo podizvajalca, ki ga je predhodno potrdil.

Za tiste nominirane podizvajalce, ki neposrednih plačil ne bodo zahtevali, bo naročnik od glavnega izvajalca zahteval, da mu najpozneje v 60 dneh od plačila končnega računa oziroma situacije pošlje svojo pisno izjavo in pisno izjavo podizvajalca, da je podizvajalec prejel plačilo za izvedena dela. Če izvajalec ne ravna skladno s tem določilom, bo naročnik Državni revizijski komisiji podal predlog za uvedbo postopka o prekršku iz 2. točke prvega odstavka 112. člena ZJN-3.

Določbe 94. člena ZJN-3 in te razpisne dokumentacije, ki urejajo izvedbo javnih naročil s podizvajalcem in varstvo podizvajalcev, ne veljajo za podizvajalce podizvajalcev glavnega izvajalca in nadaljnje podizvajalce v podizvajalski verigi.

Izbrani ponudnik v razmerju do naročnika v celoti odgovarja za izvedbo naročila.

10.2.4. Ponudba z uporabo zmogljivosti gospodarskih subjektov iz 81. člena ZJN-3

V primeru, da bo ponudnik pri izvedbi naročila uporabil zmogljivosti drugih gospodarskih subjektov iz 81. člena ZJN-3, mora v obrazcu ESPD navesti vse gospodarske subjekte, ki ponudniku zagotavljajo svoje zmogljivosti. Ponudnik mora v ponudbi predložiti tudi izpolnjene in podpisane obrazce ESPD za vsakega gospodarskega subjekta iz 81. člena ZJN-3, ter druga zahtevana dokazila o izpolnjevanju pogojev oziroma sposobnosti posameznega gospodarskega subjekta.

Pogoji, ki jih mora izpolnjevati gospodarski subjekt iz 81. člena ZJN-3, so podrobneje obrazloženi z dodatnimi pojasnili k posameznim pogojem ali v navodilih, ki so sestavni del posameznega obrazca iz te razpisne dokumentacije.

10.2.5. Ponudba, pri kateri sodeluje tuja pravna ali fizična oseba

Če je gospodarski subjekt (ponudnik, podizvajalec…) tuja pravna oseba, ki nima sedeže ali podružnice na območju Republike Slovenije, ali če je zastopnik gospodarskega subjekta tuja fizična oseba, ki nima prebivališča na območju Republike Slovenije, je potrebno predložiti potrdilo oziroma dokazilo, določeno v tej razpisni dokumentaciji, ki mora biti izdano s strani pristojnega organa države, v kateri ima gospodarski subjekt svoj sedež oziroma fizična oseba svoje prebivališče.

Če tuji gospodarski subjekt ali tuja fizična oseba ne more pridobiti in predložiti zahtevanih dokumentov, ker država v kateri ima svoj sedež oziroma prebivališče ne izdaja takšnih dokumentov, jih je mogoče nadomestiti z zapriseženo izjavo, če pa ta v državi v kateri ima gospodarski subjekt svoj sedež oziroma fizična oseba svoje prebivališče ni predvidena, pa z izjavo določene osebe, dano pred pristojnim sodnim ali upravnim organom, notarjem ali pred pristojno poklicno ali trgovinsko organizacijo v matični državi te osebe ali v državi, v kateri ima gospodarski subjekt sedež. Vzorec izjave (obrazec 6) je priloga te razpisne dokumentacije.

Potrdilom, izjavam in drugim dokumentom morajo biti priloženi prevedeni dokumenti iz tujega v slovenski jezik.

11. POGOJI ZA PRIZNANJE SPOSOBNOSTI IN DOKAZILA

11.1.

Gospodarskemu subjektu ali osebi, ki je član/ica upravnega, vodstvenega ali nadzornega organa tega gospodarskega subjekta ali ki ima pooblastila za njegovo zastopanje ali odločanje ali nadzor v njem, ni bila izrečena pravnomočna sodba za kazniva dejanja iz Kazenskega zakonika (Uradni list RS, št. 50/12 - uradno prečiščeno besedilo, 54/15, 6/16 – popr., 38/16, 27/17, 23/20, 91/20, 95/21, 186/21, 105/22 – ZZNŠPP, 16/23, 107/24 – odl. US in 1564/26; v nadaljnjem besedilu: KZ-1) ali za primerljiva kazniva dejanja, ki so jih izrekla tuja sodišča, ki so taksativno našteta v prvem odstavku 75. člena ZJN-3.

DOKAZILA:

- **Izpolnjen obrazec ESPD** *(v »Del III: Razlogi za izključitev, Oddelek A: Razlogi, povezani s kazenskimi obsodbami«)* za vse gospodarske subjekte v prijavi. V kolikor je vaš odgovor v tem primeru DA, v navedena polja vpišete podatke, ki jih od vas zahteva ESPD. V primeru, da uveljavljate popravni mehanizem, z odgovorom »Da« na vprašanje »Ste sprejeli ukrepe, s katerimi ste dokazali svojo zanesljivost ("samočiščenje")?« v polje »Prosimo opišite jih*« napišete kršitve in ukrepe, s katerimi lahko dokažete svojo zanesljivost kljub obstoju razlogov za izključitev;
- **Izpolnjen obrazec ESPD** (v »Del III: Razlogi za izključitev, Oddelek D: Nacionalni razlogi za izključitev«) za izključitveni razlog iz prvega odstavka 75. člena ZJN-3 (kršitev temeljnih pravic delavcev (196. člen KZ-1). V kolikor je vaš odgovor v tem primeru DA in uveljavljate popravni mehanizem, lahko v obrazcu ESPD (v *»Del VI. Sklepne izjave«)* ali v posebni pisni izjavi, ki jo priložite k obrazcu ESPD, navedete opis kršitev in ukrepov, s katerimi lahko dokažete svojo zanesljivost kljub obstoju razlogov za izključitev.

V primeru skupne ponudbe ali ponudbe s podizvajalci ali v primeru sklicevanja na uporabo zmogljivosti drugih gospodarskih subjektov iz 81. člena ZJN-3 mora ta pogoj izpolnjevati vsak gospodarski subjekt posamično.

Če je gospodarski subjekt v položaju iz prvega odstavka 75. člena ZJN-3, lahko najkasneje do roka za oddajo ponudb naročniku predloži dokaze, da je sprejel zadostne ukrepe, s katerimi lahko dokaže svojo zanesljivost kljub obstoju razlogov za izključitev. V tem primeru naročnik ravna v skladu z določbami devetega, desetega in enajstega odstavka 75. člena ZJN-3.

V obrazcu ESPD *(v »Del II: Informacije glede gospodarskega subjekta, Oddelek B: Informacije o predstavnikih gospodarskega subjekta«)* mora biti za vse predstavnike gospodarskega subjekta (člane upravnega, vodstvenega ali nadzornega organa) vpisana enotna matična številka občana (v nadaljnjem besedilu: EMŠO), ki naročniku omogoča preveritev podatkov v Centralni kazenski evidenci Ministrstva za pravosodje (prek sistema e-JN oziroma sistema e-Dosje).

Gospodarski subjekt, ki ima sedež v Republiki Sloveniji, lahko potrdila iz kazenske evidence Ministrstva za pravosodje priloži tudi sam. Tako predložena potrdila morajo odražati zadnje stanje, v nobenem primeru pa ne smejo biti starejša več kot štiri (4) mesece, šteto do roka za predložitev ponudb.

Za predložitev potrdil iz kazenske evidence za tuje pravne in fizične osebe, ki nimajo sedeža ali podružnice oziroma stalnega ali začasnega bivališča na območju Republike Slovenije, velja navodilo iz točke 10.2.5 tega poglavja razpisne dokumentacije.

11.2.

Gospodarski subjekt mora imeti plačane zapadle obveznosti iz naslova obveznih dajatev in drugih denarnih nedavčnih obveznosti v skladu z zakonom, ki ureja finančno upravo, ki jih pobira davčni organ v skladu s predpisi države, v kateri ima sedež, ali predpisi Republike Slovenije.

Šteje se, da gospodarski subjekt ne izpolnjuje obveznosti iz prejšnjega odstavka tudi, če davčnemu organu ni predložil vseh obračunov davčnih odtegljajev za dohodke iz delovnega razmerja za obdobje zadnjih petih let do roka za oddajo ponudbe.

Gospodarskega subjekta se ne izloči, če do roka za oddajo ponudb poravna neplačane zapadle obveznosti, ki znašajo 50 eurov ali več in davčnemu organu predloži vse obračune davčnih odtegljajev za dohodke iz delovnega razmerja za obdobje zadnjih pet let do roka za oddajo ponudbe *(drugi odstavek 75. člena ZJN-3)***.**

DOKAZILO:

- **Izpolnjen obrazec ESPD** *(v »Del III: Razlogi za izključitev, Oddelek B: Razlogi, povezani s plačilom davkov ali prispevkov za socialno varnost«)* za vse gospodarske subjekte v ponudbi.

V primeru skupne ponudbe ali ponudbe s podizvajalci ali v primeru sklicevanja na uporabo zmogljivosti drugih gospodarskih subjektov iz 81. člena ZJN-3 mora ta pogoj izpolnjevati vsak gospodarski subjekt posamično.

Za ponudnike, ki imajo sedež ali podružnico na območju Republike Slovenije, naročnik preveri podatke v uradni evidenci davčnega organa prek sistema e-JN oziroma e-Dosje.

Za predložitev potrdil iz davčne evidence ali registra druge države za tuje pravne osebe, ki nimajo sedeža ali podružnice na območju Republike Slovenije, velja navodilo iz točke 10.2.5 tega poglavja razpisne dokumentacije.

11.3.

Gospodarski subjekt na dan, ko poteče rok za oddajo ponudb, ne sme biti uvrščen v evidenco gospodarskih subjektov z izrečenimi stranskimi sankcijami izločitve iz postopkov javnega naročanja *(»a« točka četrtega odstavka 75. člena ZJN-3)***.**

DOKAZILO:

- **Izpolnjen obrazec ESPD** *(v »Del III: Razlogi za izključitev, Oddelek D: Nacionalni razlogi za izključitev«)* za vse gospodarske subjekte v ponudbi.

V primeru skupne ponudbe ali ponudbe s podizvajalci ali v primeru sklicevanja na uporabo zmogljivosti drugih gospodarskih subjektov iz 81. člena ZJN-3 mora ta pogoj izpolnjevati vsak gospodarski subjekt posamično.

Za gospodarske subjekte, ki imajo sedež ali podružnico na območju Republike Slovenije, naročnik preveri podatke v uradni evidenci pristojnega organa prek sistema e-JN oziroma e-Dosje.

Za predložitev potrdila / dokazila iz uradne evidence ali registra druge države za tuje pravne osebe, ki nimajo sedeža ali podružnice na območju Republike Slovenije, velja navodilo iz točke 10.2.5 tega poglavja razpisne dokumentacije.

11.4.

Gospodarskemu subjektu v zadnjih treh letih pred potekom roka za oddajo ponudb pristojni organ Republike Slovenije ali druge države članice ali tretje države pri njem ni ugotovil najmanj dveh kršitev v zvezi s plačilom za delo, delovnim časom, počitki, opravljanjem dela na podlagi pogodb civilnega prava kljub obstoju elementov delovnega razmerja ali v zvezi z zaposlovanjem na črno, za kateri mu je bila s pravnomočno odločitvijo ali več pravnomočnimi odločitvami izrečena globa za prekršek *(»b« točka četrtega odstavka 75. člena ZJN-3)***.**

DOKAZILO:

- **Izpolnjen obrazec ESPD** *(v »Del III: Razlogi za izključitev, Oddelek D: Nacionalni razlogi za izključitev«)* za vse gospodarske subjekte v ponudbi. V kolikor je vaš odgovor v tem primeru DA in uveljavljate popravni mehanizem, lahko v obrazcu ESPD (v *»Del VI. Sklepne izjave«)* ali v posebni pisni izjavi, ki jo priložite k obrazcu ESPD, navedete opis kršitev in ukrepov, s katerimi lahko dokažete svojo zanesljivost kljub obstoju navedenega razloga za izključitev.

Če je gospodarski subjekt v položaju iz zgornjega odstavka, lahko naročniku v skladu z devetim odstavkom 75. člena ZJN-3 najkasneje do roka za oddajo prijav predloži dokazila, da je sprejel zadostne ukrepe, s katerimi lahko dokaže svojo zanesljivost kljub obstoju razlogov za izključitev.

V primeru skupne ponudbe ali ponudbe s podizvajalci ali v primeru sklicevanja na uporabo zmogljivosti drugih gospodarskih subjektov iz 81. člena ZJN-3 mora ta pogoj izpolnjevati vsak gospodarski subjekt posamično.

Za gospodarske subjekte, ki imajo sedež ali podružnico na območju Republike Slovenije, naročnik preveri podatke v uradni evidenci pristojnega organa prek sistema e-JN oziroma e-Dosje.

Za predložitev potrdila / dokazila iz uradne evidence ali registra druge države za tuje pravne osebe, ki nimajo sedeža ali podružnice na območju Republike Slovenije, velja navodilo iz točke 10.2.5 tega poglavja razpisne dokumentacije.

11.5.

Zoper gospodarski subjekt ne sme biti začet postopek zaradi insolventnosti ali prisilnega prenehanja po zakonu, ki ureja postopek zaradi insolventnosti in prisilnega prenehanja, ali postopek likvidacije po zakonu, ki ureja gospodarske družbe, če njegova sredstva ali poslovanje upravlja stečajni oziroma likvidacijski upravitelj ali sodišče, ali če so njegove poslovne dejavnosti začasno ustavljene, ali če se je v skladu s predpisi druge države nad njim začel postopek ali pa je nastal položaj z enakimi pravnimi posledicami *(»b« točka šestega odstavka 75. člena ZJN-3)***.**

DOKAZILO:

- **Izpolnjen obrazec ESPD** (v »Del III: Razlogi za izključitev, Oddelek C: Razlogi, povezani z insolventnostjo, nasprotjem interesov ali kršitvijo poklicnih pravil«) za vse gospodarske subjekte v prijavi.

V primeru skupne ponudbe ali ponudbe s podizvajalci ali v primeru sklicevanja na uporabo zmogljivosti drugih gospodarskih subjektov iz 81. člena ZJN-3 mora ta pogoj izpolnjevati vsak gospodarski subjekt posamično.

Za gospodarske subjekte, ki imajo sedež ali podružnico na območju Republike Slovenije, naročnik preveri podatke v sodnem registru oziroma Poslovnem registru Slovenije.

Za predložitev potrdila / dokazila iz uradne evidence ali registra druge države za tuje pravne osebe, ki nimajo sedeža ali podružnice na območju Republike Slovenije, velja navodilo iz točke 10.2.5 tega poglavja razpisne dokumentacije.

11.6.

Gospodarski subjekt mora biti vpisan v enega od poslovnih registrov, ki se vodijo v državi članici, v kateri ima gospodarski subjekt sedež. Seznam poslovnih registrov v državah članicah Evropske unije določa Priloga XI Direktive 2014/24/EU *(3. odstavek 76. člena ZJN-3)***.**

DOKAZILO:

- **Izpolnjen obrazec ESPD** *(v »Del IV: Pogoji za sodelovanje, Oddelek A: Ustreznost, Vpis v poslovni register«)* s strani vseh gospodarskih subjektov v ponudbi.

V primeru skupne ponudbe ali ponudbe s podizvajalci ali v primeru sklicevanja na uporabo zmogljivosti drugih gospodarskih subjektov iz 81. člena ZJN-3 mora ta pogoj izpolnjevati vsak gospodarski subjekt posamično.

Obrazec ESPD mora vsebovati vse potrebne podatke, da lahko naročnik v uradni evidenci preveri izpolnjevanje predmetnega pogoja. V kolikor takšna preveritev ne bo mogoča, bo naročnik od gospodarskega subjekta zahteval predložitev kopije vpisa v enega od poklicnih ali poslovnih registrov.

Za gospodarske subjekte, ki imajo sedež ali podružnico na območju Republike Slovenije, naročnik preveri podatke v Poslovnem registru Slovenije.

Za predložitev potrdila / dokazila iz uradne evidence ali registra druge države za tuje pravne osebe, ki nimajo sedeža ali podružnice na območju Republike Slovenije, velja navodilo iz točke 10.2.5 tega poglavja razpisne dokumentacije.

11.7. Tehnična in funkcionalna skladnost ponujene opreme in storitev

Gospodarski subjekt mora naročniku zagotoviti opremo in storitve, ki ustrezajo vsem splošnim in tehničnim zahtevam ter specifikacijam, opredeljenim v II. poglavju razpisne dokumentacije in obrazcu 3.

DOKAZILA:

- obrazec 3 »Izjava o tehnični in funkcionalni skladnosti opreme in storitev«, s priloženo tehnično dokumentacijo, v kateri ponudnik predstavi konfiguracijo in tehnične lastnosti ponujene opreme (opisi, slike, grafikoni, prospekti, katalogi, specifikacije).

Tehnična dokumentacija proizvajalca opreme je lahko priložena v angleškem jeziku.

11.8. Kadrovska in tehnična sposobnost

Gospodarski subjekt mora zagotoviti kadrovsko in tehnično sposobnost za izvajanje storitev namestitve in konfiguracije ter garancijskega vzdrževanja ponujene opreme, oziroma izpolnjevati naslednje pogoje:

- **da ima najmanj tri (3) certificirane strokovnjake, ki imajo certifikate z napredno ravnijo tehničnega znanja za ponujene rešitve s področja mrežne varnosti, kot na primer PCNSE za Palo Alto Networks ali enakovreden certifikat drugega proizvajalca, ki ga izda proizvajalec opreme,**

- **pridobljen certifikat Cisco Preferred Security Partner (ali višji Cisco) ali enakovreden certifikat ali enakovreden status pri proizvajalcu / principalu druge ponujene enakovredne opreme;**
- **da ima za potrebe migracije najmanj dva (2) eksperta za izvajanje storitev namestitve in konfiguracije opreme za področje varnosti (kot na primer certifikat Cisco Certified Internetwork Expert - CCIE) oziroma ekvivalentni certifikat drugega proizvajalca enakovredne opreme);**
- **vsi strokovnjaki morajo aktivno govoriti slovenski jezik (nivo B2 v skladu s CEFR);**
- **gospodarski subjekt mora izkazati veljavno poslovno povezavo s principalom – proizvajalcem ponujene opreme, ki mu omogoča dostop do tehnične podpore in zagotavlja podporo pri reševanju težav v delovanju in upravljanju požarnih pregrad.**

Vsi certifikati morajo biti veljavni na dan roka za prejem ponudb. Izbrani ponudnik mora imeti ves čas trajanja pogodbe ustrezno usposobljene strokovnjake z veljavnimi certifikati. Naročnik si pridržuje pravico preveriti veljavnost certifikatov ves čas trajanja pogodbe.

DOKAZILA:
- obrazec 4 »Izjava o tehnični in kadrovski sposobnosti«,
- veljavni certifikati ali potrdila o strokovni usposobljenosti kadrov,
- dokazilo za aktivno znanje slovenskega jezika: spričevalo o izobrazbi, pridobljeni v Republiki Sloveniji, kjer je bil pouk v slovenščini (npr. matura, diploma, srednješolsko spričevalo), ali - potrdilo o opravljenem izpitu iz znanja slovenskega jezika na ustrezni ravni (B2), ki ga izdajo pooblaščene institucije, kot so: Center za slovenščino kot drugi/tuji jezik (Filozofska fakulteta UL) ali drugi javni izobraževalni zavodi, ki izvajajo preizkuse znanja jezika,
- certifikat ali pisna izjava proizvajalca strojne in programske opreme ali pooblaščenega principala, iz katere je razvidno, da ima ponudnik opreme status partnerja, ki mu omogoča dostop do tehnične podpore in zagotavlja podporo pri reševanju težav v delovanju in upravljanju požarnih pregrad.

V primeru skupne ponudbe lahko gospodarski subjekti ta pogoj izpolnjujejo kumulativno. Ponudnik se lahko sklicuje na status, certifikate in tehnično sposobnost katerega koli ponudnika - člana poslovne skupine oziroma konzorcija ali podizvajalca ali drugega gospodarskega subjekta v skladu z 81. členom ZJN-3.

V primeru skupne ponudbe lahko gospodarski subjekti ta pogoj izpolnjujejo kumulativno. Ponudnik se lahko sklicuje na kadrovske zmogljivosti katerega koli ponudnika - člana poslovne skupine oziroma konzorcija, kot tudi na zmogljivosti podizvajalca ali drugega gospodarskega subjekta v skladu z 81. členom ZJN-3.

V primeru, da ponudnik prijavi kadre, ki niso njegovi zaposleni, mora naknadno (na zahtevo naročnika) predložiti tudi dokazila o sodelovanju, iz katerih je razvidno, da bo kader s ponudnikom sodeloval pri izvajanju predmetnega naročila. To dokazilo je lahko pisni dogovor med gospodarskimi subjekti (delodajalci) ali dogovor med ponudnikom in zunanjimi kadri (npr. avtorska pogodba, podjemna pogodba ipd.).

Izbrani ponudnik je dolžan naročnika obveščati o vsaki kadrovski spremembi pri izvajanju tega naročila. Ob vsaki spremembi je potrebno predložiti dokumente, ki so zahtevani in se štejejo za usposobljenost kadra. Kot sprememba se štejejo morebitni dodatni kadri, ki bi opravljali predmetne storitve, kot tudi morebitna zamenjava v ponudbi prijavljenega kadra. Naročnik si pridržuje pravico kadar koli v času trajanja pogodbe preveriti izpolnjevanje kadrovskih pogojev.

11.9. Reference

Gospodarski subjekt mora predložiti najmanj tri (3) referenčna potrdila, da je v zadnjih treh (3) letih pred iztekom roka za predložitev ponudbe, po pravilih stroke, pravočasno in kakovostno dobavil in konfiguriral vsaj dve (2) požarni pregradi v visoko razpoložljivostnem načinu delovanja, pri čemer je bil vsak od treh izvedenih poslov v vrednosti najmanj 50.000,00 EUR brez DDV in pri katerih omrežje, ki vključuje te naprave, uporablja najmanj 250 uporabnikov.

DOKAZILO:

- **Izpolnjen obrazec ESPD** *(v »Del IV: Pogoji za sodelovanje, Oddelek C: Tehnična in strokovna sposobnost, Za naročila blaga: Izvedba dobave blaga določene vrste«);*
- potrdilo referenčnega naročnika (obrazec 5).

V primeru skupne ponudbe lahko ponudniki ta pogoj izpolnjujejo kumulativno. Ponudnik se lahko sklicuje na reference katerega koli ponudnika - člana poslovne skupine oziroma konzorcija, kot tudi na reference podizvajalca ali drugega gospodarskega subjekta v skladu z 81. členom ZJN-3.

Ponudniku, partnerju v skupni ponudbi in podizvajalcu se ne bodo upoštevale reference, ki bi si jih ti subjekti potrdili en drugemu, kot naročniki referenčnega posla. Upoštevale se bodo reference, ki jih bo potrdil glavni naročnik referenčnega posla, ki pa ni ponudnik, partner ali podizvajalec sam ali naročnik, za katerega se glede na določbe zakona, ki ureja gospodarske družbe (ZGD-1) šteje, da je z njimi povezana družba.

Naročnik si pridržuje pravico, da od ponudnika naknadno zahteva dodatna dokazila o izvedbi referenčnega naročila (na primer: pogodbo ali naročilnico z referenčnim naročnikom) oziroma, da navedbe preveri neposredno pri referenčnem naročniku.

11.10. Finančno zavarovanje

Gospodarski subjekt mora naročniku zagotoviti, da bo v primeru izbire oziroma izvedbe javnega naročila sposoben v roku 8 dni po sklenitvi pogodbe predložiti finančno zavarovanje za dobro izvedbo pogodbenih obveznosti in odpravo napak v garancijskem roku v višini 10 % skupne pogodbene vrednosti z DDV, veljavno od dneva izdaje in še 30 dni po prenehanju pogodbe, skladno z vzorcem iz razpisne dokumentacije. Finančno zavarovanje za dobro izvedbo pogodbenih obveznosti in odpravo napak v garancijskem roku mora biti brezpogojno in plačljivo na prvi poziv.

DOKAZILO:

- izjava ponudnika, ki je sestavni del obrazca 2 »Ponudba / Predračun«.

Ponudnik, ki bo izbran (v nadaljnjem besedilu: glavni izvajalec), mora v roku 8 dni po podpisu pogodbe predložiti naročniku tri (3) menice in menično izjavo, kot finančno zavarovanje za dobro izvedbo pogodbenih obveznosti in odpravo napak v garancijskem roku.

Finančno zavarovanje oziroma vsebino menične izjave podrobneje ureja vzorec pogodbe, ki je sestavni del razpisne dokumentacije.

V primeru, da bo javno naročilo oddano ponudnikom, ki so oddali skupno ponudbo, se finančno zavarovanje predloži ob sklenitvi pogodbe na način, da ga predloži samo eden izmed skupnih ponudnikov ali vsak ponudnik posebej. V kolikor je finančno zavarovanje predloženo s strani vsakega izmed ponudnikov, mora biti seštevek vseh zneskov zavarovanj najmanj v višini zahtevanega zneska.

Naročnik bo unovčil menice v primerih, določenih v vzorcu pogodbe, pri čemer skupna vrednost vseh unovčenih menic ne bo presegla 10 % celotne pogodbene vrednosti z DDV.

S predložitvijo obrazca 2 »Ponudba / Predračun« se šteje, da ponudnik sprejema pogoje finančnega zavarovanja, določene v vzorcu pogodbe, ter da sprejema vse pravice in obveznosti iz naslova finančnega zavarovanja, določene v razpisni dokumentaciji oziroma v vzorcu pogodbe.

Predložitev finančnega zavarovanja je pogoj za veljavnost pogodbe.

12. MERILO ZA OCENJEVANJE PONUDB IN IZBIRO PONUDNIKA

Merilo je ekonomsko najugodnejša ponudba, določena na podlagi najnižje skupne ponudbene cene za opremo in storitve v EUR z DDV.

Ponudnik, ki izpolnjuje vse pogoje za priznanje sposobnosti in ponudi najnižjo skupno ceno za opremo in storitve, je najugodnejši ponudnik in bo izbran za dobavitelja opreme oziroma izvajalca storitev, ki so predmet tega javnega naročila.

V primeru, da bosta dva ali več ponudnikov ponudila enako najnižjo ponudbeno ceno za opremo in storitve v EUR z DDV, bo naročnik izbral ponudnika, ki je prej oddal ponudbo.

13. DRUGA DOLOČILA ZA PRIPRAVO PONUDBE

13.1. Ponudbena dokumentacija

Ponudbeno dokumentacijo sestavljajo naslednji dokumenti:

- obrazec 1 »ESPD« (za vse gospodarske subjekte v ponudbi);
- obrazec 2 »Ponudba / Predračun« (izpolnjen obrazec v PDF datoteki), ki ga ponudnik v informacijskem sistemu e-JN pripne oziroma naloži v razdelek »Predračun« tako, da bo obrazec razkrit/dostopen na javnem odpiranju ponudb;
- obrazec 3 »Izjava o tehnični in funkcionalni skladnosti opreme in storitev«, s priloženo tehnično dokumentacijo, navedeno v točki 11.7. razpisne dokumentacije;
- obrazec 4 »Izjava o tehnični in strokovni sposobnosti«; s prilogami oziroma certifikati, potrdili in dokazili, navedenimi v točki 11.8. razpisne dokumentacije;
- obrazec 5 »Potrdilo referenčnega naročnika«;
- potrdila za tuje pravne in fizične osebe, ki nimajo sedeža ali podružnice oziroma stalnega ali začasnega prebivališča na območju Republike Slovenije, skladno z navodilom naročnika iz točke 10.2.5 te razpisne dokumentacije, in sicer:
    - potrdilo pristojnega organa tuje države, ki vodi kazensko evidenco iz točke 11.1 te razpisne dokumentacije, ali izpolnjen obrazec 6 »Izjava tuje fizične osebe o nekaznovanosti«;
    - potrdilo pristojnega davčnega organa tuje države, ki vodi uradno evidenco iz točke 11.2 te razpisne dokumentacije);
    - potrdilo pristojnega organa tuje države, ki vodi uradno evidenco iz točke 11.4 te razpisne dokumentacije;

- potrdilo pristojnega organa tuje države, ki vodi uradno evidenco iz točke 11.5 te razpisne dokumentacije;
- izpisek iz registra ali potrdilo pristojnega organa tuje države, ki vodi register iz točke 11.6 te razpisne dokumentacije.

V primeru obstoja izključitvenega razloga in v kolikor gospodarski subjekt uveljavlja popravni mehanizem, ki ni naveden oziroma obrazložen v obrazcu ESPD (v *»Del VI. Sklepne izjave«),* se k ponudbi priloži pisna izjava, v kateri gospodarski subjekt navede opis kršitev in ukrepov, s katerimi dokazuje svojo zanesljivost kljub obstoju razloga za izključitev.

Opozorilo!
Gospodarski subjekt pod kazensko in materialno odgovornostjo jamči, da so vsi podatki in dokumenti ter izjave, podane v ponudbi, resnični, in da kopije priloženih listin ustrezajo izvirniku. V nasprotnem primeru je gospodarski subjekt odgovoren za sankcije za prekrške, določene v 110. in 112. členu ZJN-3 (v povezavi z 11. odstavkom 89. člena ZJN-3), ter naročniku odgovarja za vso škodo, ki mu je nastala.

13.2. Obrazec ESPD za vse gospodarske subjekte

Obrazec ESPD predstavlja uradno izjavo gospodarskega subjekta, da zanj ne obstajajo razlogi za izključitev in da izpolnjuje pogoje za sodelovanje, hkrati pa zagotavlja ustrezne informacije, ki jih zahteva naročnik. Obrazec ESPD vključuje tudi uradno izjavo o tem, da bo gospodarski subjekt na zahtevo in brez odlašanja sposoben predložiti dokazila, ki dokazujejo neobstoj razlogov za izključitev oziroma izpolnjevanje pogojev za sodelovanje.

Navedbe v ESPD in/ali dokazila, ki ji predloži gospodarski subjekt, morajo biti veljavni.

Gospodarski subjekt naročnikov obrazec ESPD (datoteka XML) uvozi na spletni povezavi: https://ejn.gov.si/espd in v njega neposredno vnese zahtevane podatke.

Podrobnejše informacije in navodila za izpolnjevanje obrazca ESPD so gospodarskim subjektom dostopna v dokumentu *»Navodila za uporabo enotnega evropskega dokumenta v zvezi z oddajo javnega naročila – ESPD za ponudnike«,* ki je objavljen na spletnem naslovu, navedenem v prejšnjem odstavku oziroma Navodila in obrazci (gov.si).

Izpolnjen in podpisan ESPD mora biti v prijavi priložen za vse gospodarske subjekte, ki v kakršni koli vlogi sodelujejo v ponudbi (ponudnik, sodelujoči ponudnik v primeru skupne prijave, gospodarski subjekti, na katerih kapacitete se sklicuje ponudnik in podizvajalci).

Ponudnik, ki v sistemu e-JN oddaja prijavo, naloži svoj ESPD v razdelek »Dokumenti«, del »ESPD – ponudnik«, ESPD ostalih sodelujočih pa naloži v razdelek »Sodelujoči«, del »ESPD – ostali sodelujoči«. Ponudnik, ki v sistemu e-JN oddaja ponudbo, naloži elektronsko podpisan ESPD v xml. obliki ali nepodpisan ESPD v xml. obliki, pri čemer se v slednjem primeru v skladu Splošnimi pogoji uporabe sistema e-JN šteje, da je oddan pravno zavezujoč dokument, ki ima enako veljavnost kot podpisan.

Za ostale sodelujoče ponudnik, ki v sistemu e-JN oddaja ponudbo, v razdelek »Sodelujoči«, del »ESPD – ostali sodelujoči« priloži ESPD v pdf. obliki, ki mora biti elektronsko podpisan ali lastnoročno podpisan in skeniran obrazec, ali v elektronski obliki podpisan xml.

13.3. Obrazec »Ponudba / Predračun«

Ponudnik mora izpolniti vse postavke v razpredelnici.

Cena za posamezno postavko oziroma enoto in skupna ponudbena cena za celotno količino mora biti izražena v evrih (EUR) in sicer na največ dve decimalni mesti.

Če ponudnik cene v posamezno postavko ne vpiše, se šteje, da predmetne postavke ne ponuja in tako ne izpolnjuje vseh zahtev naročnika iz predmetne razpisne dokumentacije.

Če ponudnik vpiše ceno nič (0 ali 0,00) EUR, se šteje, da ponuja postavko brezplačno.

Cena mora vsebovati vse stroške, ki se neposredno ali posredno nanašajo na dobavo opreme in izvajanje vseh predmetnih storitev (vključno s storitvami in stroški proizvajalca licenčne programske opreme). V skupnem znesku ponudbe oziroma predračuna morajo biti upoštevani naslednji stroški:

- kupnina za opremo in licence z vštetim garancijskim vzdrževanjem strojne opreme,
- cena delovne ure serviserja, pripravljenost, potni stroški, čas servisiranja itd.,
- zagotavljanje odzivnega časa in popravila v zahtevanem režimu vzdrževanja,
- stroški rezervnih delov in nadomestne opreme,
- stroški potrošnega materiala in medijev potrebnih za izvedbo vzdrževanja,
- stroški skladiščenja priporočenih rezervnih delov in opreme, ki omogoča zamenjavo v zahtevanem režimu,
- stroški, povezani z nadgradnjo in novimi verzijami programske opreme,
- sistemsko konfiguriranje,
- pomoč po telefonu,
- usposabljanje uporabnikov opreme, zaposlenih pri naročniku,
- zagotavljanje uporabniške dokumentacije,
- zagotavljanje garancij za rezervne dele, opremo in opravljene storitve,
- stroški, povezani z zagotavljanjem ustreznih finančnih zavarovanj za dobro izvedbo pogodbenih obveznosti in odpravo napak v garancijskem roku, skladno z vzorcem pogodbe, ki je sestavni del razpisne dokumentacije,
- davek na dodano vrednost,
- drugi stroški, ki se neposredno ali posredno nanašajo na dobavo, namestitev, konfiguracijo in vzdrževanje opreme.

Stroški 36-mesečnega garancijskega vzdrževanja strojne opreme so brezplačni oziroma všteti v ceno/kupnino strojne opreme.

Naročnik stroškov, ki niso zajeti v ponudbeni ceni, naknadno ne bo priznaval.

Cene na enoto (za blago in storitve), izražene v EUR brez DDV, morajo biti fiksne.

Ponudnik ne sme spreminjati vsebine predračuna.

Ponudnik v sistem e-JN v razdelek »Skupna ponudbena vrednost« v zato namenjen prostor vpiše skupni ponudbeni znesek brez davka v EUR in znesek davka v EUR. Znesek skupaj z davkom v EUR se izračuna samodejno. V del »Predračun« pa naloži datoteko v obliki PDF. »Skupna ponudbena vrednost«, ki bo vpisana v istoimenski razdelek in dokument, ki bo naložen kot predračun v del »Predračun«, bosta razvidna in dostopna na javnem odpiranju ponudb.

V primeru razhajanj med podatki navedenimi v razdelku »Skupna ponudbena vrednost« in dokumentu, ki je predložen v delu »Predračun«, kot veljavni štejejo podatki v dokumentu, ki je predložen v delu »Predračun«.

Če bo naročnik pri pregledu in ocenjevanju ponudb odkril očitne računske napake, bo ravnal v skladu s sedmim odstavkom 89. člena ZJN-3.

Če je oddana skupna ponudba več ponudnikov ali če pri ponudbi sodelujejo podizvajalci ali drugi gospodarski subjekti iz 81. člena ZJN-3, si naročnik pridržuje pravico, da od ponudnika, ki je oddal dopustno in ekonomsko najugodnejšo ponudbo, naknadno zahteva predložitev kalkulacije ponudbene cene, razčlenjene po posameznih gospodarskih subjektih, ter pogodb in drugih aktov, ki urejajo medsebojna obligacijska razmerja med gospodarskimi subjekti pri izvedbi javnega naročila.

13.4. Obrazec 3 »Izjava o tehnični in funkcionalni skladnosti opreme in storitev«

Gospodarski subjekt k ponudbi priloži izpolnjen obrazec 3 »Izjava o tehnični o tehnični in funkcionalni skladnosti opreme in storitev« s tehnično dokumentacijo, navedeno v točki 11. 7. razpisne dokumentacije.

Tehnična dokumentacija proizvajalca opreme je lahko priložena v angleškem jeziku.

13.5. Obrazec 4 »Izjava o tehnični in strokovni sposobnosti«

Gospodarski subjekt k ponudbi priloži izpolnjen obrazec 4 »Izjava o tehnični in strokovni sposobnosti« z dokazili, navedenimi v točki 11.8 razpisne dokumentacije.

13.6. Obrazec 5 »Referenčno potrdilo«

Gospodarski subjekt k ponudbi priloži najmanj 3 (tri) referenčna potrdila, podpisana s strani referenčnih naročnikov.

13.7. Ostale priloge

Gospodarski subjekt, ki v sistemu e-JN oddaja ponudbo, mora ostale dokumente ponudbene dokumentacije, ki so navedeni v točki 13.1 te razpisne dokumentacije, naložiti v informacijski sistem e-JN v razdelek »Dokumenti«, del »Ostale priloge«.

Posamezne priloge oziroma datoteke so lahko združene v eno ZIP datoteko.

13.8. Jezik, v katerem mora ponudnik pripraviti ponudbo

Postopek javnega naročanja poteka v slovenskem jeziku, vključno z vprašanji, ki jih naročniku posredujejo ponudniki prek portala javnih naročil. Vsi dokumenti v zvezi s ponudbo morajo biti v slovenskem jeziku. Potrdilom, izjavam, dokazilom in drugim dokumentom, ki so v tujem jeziku, morajo biti priloženi s strani prevajalca prevedeni dokumenti.

Ne glede na prejšnji odstavek lahko ponudnik predloži certifikate in tehnično dokumentacijo v angleškem jeziku. Če naročnik ob pregledu in ocenjevanju ponudb meni, da je potrebno del tehnične dokumentacije ali ponudbe, ki ni predložen v slovenskem jeziku, prevesti v slovenski jezik, lahko od ponudnika zahteva, da le-to stori na lastne stroške, ter mu za to določi ustrezen rok. Če ponudnik v roku, ki ga določi naročnik, ne predloži prevoda, bo naročnik njegovo ponudbo kot nepopolno izločil iz nadaljnjega postopka. Za presojo spornih vprašanj se vedno uporablja ponudba v slovenskem jeziku in del ponudbe v overjenem prevodu v slovenski jezik.

13.9. Obseg ponudbe

Ponudnik poda ponudbo kot celoto.

Ponudbe po sklopih ali variantne ponudbe niso dovoljene in jih naročnik ne bo upošteval.

13.10. Rok veljavnosti ponudbe

Ponudba mora veljati najmanj 3 mesece od dneva oddaje prek sistema e-JN. V primeru krajšega roka veljavnosti ponudbe se ponudba izloči.

Zaradi morebitnega revizijskega zahtevka ali drugih objektivnih okoliščin, ki nastanejo v roku

veljavnosti ponudbe, lahko naročnik zahteva od ponudnikov podaljšanje roka za veljavnost oddane ponudbe, vendar ne več kot za 90 dni.

13.11. Stroški ponudbe

Vse stroške, povezane s pripravo in predložitvijo ponudbe, nosi ponudnik.

13.12. Označitev zaupnih podatkov

Ponudnik mora v svoji ponudbi označiti tiste podatke in dokumente ali dele dokumentov, ki izpolnjujejo pogoje in zahteve za poslovno skrivnost v skladu z 2. členom Zakona o poslovni skrivnosti (Uradni list RS, št. 22/19; v nadaljnjem besedilu: ZPosS) ali k ponudbi priložiti pisni sklep ali drug akt o določitvi poslovne skrivnosti.

Če je zaupen samo določen podatek (beseda, številka, stavek ali odstavek) v obrazcu ali dokumentu, mora biti zaupni podatek ali del dokumenta podčrtan ali osenčen, v isti vrstici ob desnem robu pa oznaka »POSLOVNA SKRIVNOST« ali druga varnostna oznaka, ki jo ponudnik uporablja v skladu s svojimi notranjimi akti, ki urejajo varovanje poslovne skrivnosti. Pri tem ni dovoljeno neopravičeno ali pavšalno označevati zaupnosti celotne ponudbe in tistih dokumentov, ki so javnega značaja, skladno s 35. členom ZJN-3 in tretjim odstavkom 2. člena ZPosS. V primeru, da bodo kot poslovna skrivnost označeni podatki, ki ne ustrezajo pogojem, bo naročnik ponudnika pozval, da oznako zaupnosti ali poslovna skrivnost umakne. Če ponudnik v roku, ki ga določi naročnik ne prekliče zaupnosti, naročnik ponudbo izloči.

V kolikor ponudnik ne označi poslovne skrivnosti v pisni obliki, se šteje, da je celotna ponudba javna na način ter pod pogoji, določenimi v 35. členu ZJN-3 in Zakonu o dostopu do informacij javnega značaja (Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 117/06 – ZDavP-2, 23/14, 50/14, 19/15 –odl. US, 102/15, 7/18, 141/22 in 40/25 – ZInfV-1).

13.13. Sprememba ali dopolnitev ponudbe

Dopolnitve, popravki, spremembe ali pojasnila ponudbe ter popravki računskih napak so dopustni v obsegu, na način in pod pogoji, ki so določeni v 89. členu ZJN-3.

13.14. Protikorupcijska določba

V postopku oddaje javnega naročila naročnik in ponudniki ne smejo pričenjati in izvajati dejanj, ki bi vnaprej določila izbor določene ponudbe, ali ki bi povzročila, da pogodba ne bi pričela veljati oziroma ne bi bila izpolnjena.
Vsakršno lobiranje v postopkih oddaje javnih naročil je prepovedano.

Javni uslužbenci UJP, ki vodijo postopek oddaje javnega naročila ali sodelujejo pri pripravi razpisne dokumentacije ali njenih delov ali na kateri koli stopnji odločajo v postopku javnega naročanja, morajo generalnega direktorja UJP obvestiti o morebitnem korupcijskem tveganju in nasprotju interesov v primerih in pod pogoji, določenimi v 91. členu ZJN-3, in sicer takoj po odpiranju ponudb oziroma najpozneje pred sprejemom poročila in predloga za oddajo javnega naročila.

Protikorupcijska klavzula je podrobneje urejena v vzorcu pogodbe, ki je sestavni del te razpisne dokumentacije.

14. DAJANJE NERESNIČNIH ALI ZAVAJAJOČIH IZJAV IN DOKAZIL

Če se pri naročniku v postopku javnega naročanja pojavi utemeljen sum, da je ponudnik predložil neresnično izjavo ali ponarejeno ali spremenjeno listino kot pravo, bo Državni revizijski komisiji podal predlog za uvedbo postopka o prekršku, kot to določa 11. odstavek 89. člena ZJN-3.

15. USTAVITEV POSTOPKA IN ODSTOP OD IZVEDBE JAVNEGA NAROČILA

UJP lahko do roka za oddajo ponudb kadar koli ustavi postopek oddaje javnega naročila, skladno s prvim odstavkom 90. člena ZJN-3.

UJP lahko na vseh stopnjah postopka po izteku roka za odpiranje ponudb zavrne vse ponudbe, skladno s petim odstavkom 90. člena ZJN-3.

UJP lahko na podlagi osmega odstavka 90. člena ZJN-3 po sprejemu odločitve o oddaji naročila do sklenitve pogodbe odstopi od izvedbe javnega naročila iz utemeljenih razlogov, da predmeta javnega naročila ne potrebuje več ali da zanj nima zagotovljenih sredstev ali da se pri naročniku pojavi utemeljen sum, da je bila ali bi lahko bila vsebina pogodbe posledica storjenega kaznivega dejanja, ali da so nastale druge izredne okoliščine, na katere naročnik ni mogel vplivati in jih predvideti ter zaradi katerih je postala izvedba javnega naročila z izbranim ponudnikom nemogoča. V tem primeru bo UJP o svoji odločitvi in o razlogih, zaradi katerih odstopa od izvedbe javnega naročila, pisno obvestil ponudnika.

UJP objavi odločitev o ustavitvi postopka oddaje javnega naročila ali zavrnitvi vseh ponudb ali odstopu od izvedbe javnega naročila na portalu javnih naročil.

UJP ne odgovarja za škodo, ki bi utegnila nastati ponudnikom zaradi ustavitve postopka, zavrnitve vseh ponudb ali izbranemu ponudniku zaradi ne sklenitve pogodbe.

16. OBVESTILO O ODLOČITVI O ODDAJI NAROČILA

UJP bo odločitev o oddaji naročila objavil na portalu javnih naročil, skladno z desetim odstavkom 90. člena ZJN-3. Odločitev se šteje za vročeno z dnem objave na portalu javnih naročil.

UJP lahko do pravnomočnosti odločitve o oddaji javnega naročila z namenom odprave nezakonitosti svojo odločitev na lastno pobudo spremeni in sprejme novo odločitev, s katero nadomesti prejšnjo, skladno s šestim odstavkom 90. člena ZJN-3.

17. POGODBA

Izbrani ponudnik bo po pravnomočnosti odločitve o oddaji javnega naročila pozvan k podpisu pogodbe. Izbrani ponudnik mora v roku osmih (8) delovnih dni od prejema s strani naročnika podpisane pogodbe le to podpisati in jo vrniti naročniku, v nasprotnem primeru se šteje, da umika svojo ponudbo in da odstopa od podpisa pogodbe.

Naročnik si pridržuje pravico, da vzorec pogodbe pred podpisom vsebinsko prilagodi oziroma dopolni tako, da posamezne določbe razpisne dokumentacije prenese v ustrezne člene ali poglavja pogodbe, ali zaradi morebitnih uskladitev, glede na to ali bo izbrani ponudnik predložil skupno ponudbo ali prijavil sodelovanje podizvajalcev ter glede na način podpisa (lastnoročni ali elektronski podpis).

Naročnik in izbrani ponudnik lahko sporazumno določita izvedbene akte (protokol, sporazum, uporabniška navodila, poročila, zapisniki, obrazci ipd.), v katerih se podrobneje določi način izvajanja posameznih pogodbenih obveznosti.

Naročnik si pridržuje pravico, da po sklenitvi pogodbe zahteva spremembo pogodbe ali odstopi od pogodbe na način ter pod pogoji, določenimi v pogodbi ter v 95. in 96. členu ZJN-3.

18. VARSTVO OSEBNIH PODATKOV

V postopku oddaje tega javnega naročila ter pri izvajanju pogodb bo zagotovljeno varstvo osebnih podatkov v skladu z določbami Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L št. 119 z dne 4. 5. 2016, str. 1; v nadaljnjem besedilu: Splošna uredba o varstvu podatkov ali GDPR) in Zakona o varstvu osebnih podatkov (Uradni list RS, št. 163/22, 40/25–ZInfV-1 in 10/26 – ZP-1L; v nadaljnjem besedilu: ZVOP-2).

Postopki in organizacijski ter tehnični ukrepi za varovanje osebnih podatkov so podrobneje določeni v notranjih aktih naročnika, ki urejajo ravnanje z dokumentarnim gradivom, varovanje podatkov oziroma informacijsko varnost, revizijske sledi, upravljanje in vzdrževanje strojne in sistemske aplikativne programske opreme ter druge informacijske infrastrukture, fizično in tehnično varovanje prostorov in opreme.

Naročnik v zvezi z oddajo in izvajanjem tega javnega naročila obdeluje osebne podatke o osebah, ki jih gospodarski subjekti navedejo v svojih ponudbah ali priloženi dokumentaciji (lastniki, zastopniki, prokuristi, člani uprave, člani nadzornega organa, skrbniki pogodb, kontaktne osebe, podizvajalci, podatki referenčnih naročnikov ipd.), in sicer:

- podatki o lastnikih gospodarskih subjektov: osebno ime, naslov stalnega ali začasnega prebivališča - ulica, hišna številka, kraj, poštna številka, država, višina denarnega vložka v EUR, delež lastništva v %;
- podatki o osebah, ki so člani upravnega, vodstvenega ali nadzornega organa gospodarskega subjekta: osebno ime in prejšnje osebno ime, datum, kraj, občina in država rojstva, EMŠO, naslov stalnega ali začasnega prebivališča (ulica, hišna številka, kraj, poštna številka, država), državljanstvo, funkcija ali delovno mesto v gospodarskem subjektu, podatki o nekaznovanosti za kazniva dejanja, ki so taksativno našteta v prvem odstavku 75. člena ZJN-3;
- kontaktni podatki oseb, odgovornih za pripravo ponudbe ali skrbništvo pogodbe: osebno ime, delovno mesto, telefon, elektronski naslov;
- podatki o osebah, ki opravljajo delo po pogodbi v okviru javnega naročila: osebno ime, delovno mesto, delodajalec (naziv in sedež), vrsta in stopnja strokovne izobrazbe, dodatna funkcionalna znanja in strokovni izpiti (potrdila in certifikati), delovne izkušnje, opis nalog v okviru javnega naročila, delovno dovoljenje (če je delavec tujec), kontaktni podatki (telefon, telefaks, e-naslov);
- kontaktni podatki iz referenčnih potrdil drugih naročnikov: osebno ime, delovno mesto, telefon, elektronski naslov, naziv in naslov referenčnega naročnika;
- kontaktni podatki, navedeni v izdanih e-računih ali njihovih prilogah: osebno ime, delovno mesto, telefon, elektronski naslov.

Splošne informacije o varstvu osebnih podatkov v UJP in pravicah posameznikov, na katere se nanašajo osebni podatki, ter kontaktni podatki pooblaščene osebe za varstvo osebnih podatkov, so dostopni na spletni strani UJP O Upravi Republike Slovenije za javna plačila | GOV.SI.

19. PRAVNO VARSTVO

Zahtevek za revizijo, ki se nanaša na vsebino objave in/ali razpisno dokumentacijo, se lahko vloži v desetih (10) delovnih dneh od dneva objave obvestila o javnem naročilu ali obvestila o dodatnih informacijah in informacijah o nedokončanem postopku ali popravku, če se s tem obvestilom spreminjajo ali dopolnjujejo zahteve ali merila za izbor najugodnejšega ponudnika, pri čemer se lahko zahtevek za revizijo nanaša na spremenjeno, dopolnjeno ali pojasnjeno vsebino objave ali razpisne

dokumentacije ali z njim neposredno povezano navedbo v prvotni objavi ali razpisni dokumentaciji. Zahtevka za revizijo ni dopustno vložiti po roku za prejem ponudb.

Zahtevek za revizijo mora vsebovati vse podatke in dokazila, kot jih določa 15. člen Zakona o pravnem varstvu v postopkih javnega naročanja (Uradni list RS, št. 43/11, 60/11 – ZTP-D, 63/13, 90/14 – ZDU-1I, 60/17, 72/19 in 83/25 - ZOUL; v nadaljnjem besedilu: ZPVPJN).

Takso v višini 2.000,00 EUR mora vlagatelj plačati na transakcijski račun Ministrstva za finance, številka IBAN SI56 0110 0100 0358 802, BIC koda banke prejemnika: BSLJSI2X – *»taksa za postopek revizije javnega naročanja«.* Pri tem mora na plačilnem nalogu vpisati naslednje podatke v predpolje in polje sklicevanja na številko odobritve: 11 16110-7111290-04308626.

Zahtevek za revizijo mora biti vložen prek portala e-Revizije, skladno s 13.a členom ZPVPJN in določbami Pravilnika o portalu e-Revizija za izmenjavo informacij in dokumentov v predrevizijskem, revizijskem in pritožbenem postopku (Uradni list RS, št. 32/19, 67/20 in 92/25).

Informacije o pravnem varstvu zoper odločitev naročnika, sprejeto v skladu z 90. členom ZJN-3, bodo navedene v odločitvi naročnika, ki bo ponudnikom vročena prek portala javnih naročil.

Podrobnejše informacije o pravnem varstvu in izmenjavi dokumentov ter podatkov v postopku pravnega varstva so dostopne na spletni strani portala e-Revizija https://www.portalerevizija.si/ in spletni strani Ministrstva za notranje zadeve in javno upravo https://www.gov.si/teme/pravno-varstvo-v-postopkih-javnega-narocanja/.

Urška Kos
generalna direktorica

II. PREDMET JAVNEGA NAROČILA IN TEHNIČNE ZAHTEVE

1. Opis trenutnega komunikacijskega omrežja

Trenutno naročnikovo komunikacijsko omrežje sestavljata dve stateful požarni pregradi proizvajalca Cisco Systems, Inc., (Cisco ASA), ki delujeta v režimu visoke razpoložljivosti (angl. HA). Požarni pregradi izvajata filtriranje prometa do nivoja Layer 4, pri čemer se filtriranje paketov izvaja na podlagi vnaprej določenih pravil dostopa (angl. ACL). Poleg tega požarni pregradi delujeta tudi kot VPN koncentratorja za oddaljeni dostop 150 uporabnikov naročnika (RAVPN).

2. Predmet javnega naročila

Predmet javnega naročila je dobava dveh (2) kompletov požarnih pregrad za nadgradnjo v obstoječem komunikacijskem omrežju naročnika. Na perimetru komunikacijskega omrežja sta dve požarni pregradi proizvajalca Cisco Systems, Inc., katerima se zaradi dotrajanosti strojne opreme izteka življenjski cikel. Z novima požarnima pregradama bo naročnik pridobil napredne varnostne mehanizme filtriranja in možnost vpogleda v omrežni promet. Z zamenjavo požarnih pregrad se zvišuje nivo varnosti komunikacijskega omrežja naročnika.

2.1. Splošne zahteve

Ponudnik mora dobaviti 2 kompleta požarnih pregrad, na primer Palo Alto PA-560, z zahtevanimi lastnostmi in zmogljivostmi, opisanimi v nadaljevanju.

Oprema mora omogočati oddaljeni dostop za 150 uporabnikov naročnika (RAVPN).

Ponujena oprema mora biti funkcionalno in protokolno združljiva z obstoječim komunikacijskim omrežjem naročnika, tehnično preverjena ter mora zagotavljati zanesljivo delovanje v obstoječem sistemu oziroma omrežju.

Oprema mora biti skladna z zahtevano konfiguracijo, namenjena slovenskemu trgu ter opremljena z vsemi potrebnimi veljavnimi atesti in dovoljenji za uporabo v Republiki Sloveniji. Omogočati mora uporabo in vzdrževanje v Sloveniji brez dodatnih prilagoditev ali sprememb.

Vsa strojna oprema mora biti nova in proizvedena v letu 2026.

Ponudnik mora biti pooblaščen serviser ponujene opreme ter mora zagotavljati rezervne dele za vso ponujeno opremo v zahtevani konfiguraciji najmanj pet (5) let od dneva primopredaje opreme.

2.2. Tehnične zahteve in lastnosti obeh požarnih pregrad

Navedene lastnosti in zmogljivosti veljajo za dve požarni pregradi:

2.2.1. Splošne lastnosti:

1. požarna pregrada mora omogočati aplikacijsko pregledovanje in nadziranje prometa (angl. NGFW požarna pregrada),
2. požarna pregrada mora imeti zasnovo primerno za okolja z visoko zanesljivostjo (active/passive HA),

3. požarna pregrada mora biti namenska naprava (virtualna naprava ni sprejemljiva),
4. proizvajalec požarne pregrade se mora nahajati v četrtem (leader) kvadrantu Gartner poročil za Next-Generation požarne pregrade vsaj zadnjih 5 let,
5. postavitev požarne pregrade mora omogočati naslednje scenarije:
   - transparentni prehod za prestrezanje (Virtual Wire),
   - L3 način (požarna pregrada je privzeti prehod napravam v omrežju),
   - zajem kopije prometa za analizo (tap),
   - L2 način,

6. požarna pregrada mora imeti fizično ločeno upravljalno ravnino (angl. Management plane), ki skrbi za grafični vmesnik in konfiguracijo, ter podatkovno ravnino (angl. Data plane), ki obravnava promet, ki poteka skozi požarno pregrado. Poleg tega mora imeti požarna pregrada najmanj 2 CPU jedri, namenjeni izključno upravljalni ravnini,
7. požarna pregrada mora imeti fizično ločen upravljalni vmesnik (out-of-band management), ki omogoča popolno izolacijo upravljanja od produkcijskega prometa.

2.2.2. Tehnične zmogljivosti:

1. požarna pregrada mora biti strojna, namenska naprava, optimizirana z ustreznimi pospeševalnimi komponentami (npr. ASIC, FPGA), tako da vse NGFW storitve izvaja pospešeno na namenski strojni opremi; poizvedbe na upravljalni ravnini pri tem ne smejo vplivati na pretočni oziroma podatkovni del,
2. požarna pregrada mora omogočati vsaj 8,5 Gbps prepustnosti pri aplikacijskem pregledovanju in nadzoru vsega prometa,
3. požarna pregrada mora omogočati vsaj 6 Gbps prepustnosti pri aplikacijskem pregledovanju in nadzoru vsega prometa ter pri vključenih vseh varnostnih preverjanjih prometa (angl. Threat Prevention Throughput). Navedena zahteva se ne nanaša zgolj na prepustnost pri varnostnih preverjanjih, ki so predmet tega naročila, temveč mora biti zagotovljena tudi ob morebitnem kasnejšem dodajanju novih varnostnih preverjanj,
4. požarna pregrada mora omogočati vsaj 5,5 Gbps prepustnosti pri prometu IPSec VPN, najmanj 598.000 sočasnih sej, najmanj 100.000 novih sej na sekundo ter najmanj 10 virtualnih usmerjevalnikov (npr. VRF),
5. požarna pregrada mora podpirati virtualizacijo oziroma razdelitev na najmanj pet (5) virtualnih razdelkov z neodvisnimi vmesniki in politikami ter že vključevati možnost uporabe vsaj enega (1) virtualnega razdelka (virtualni sistemi, konteksti),
6. požarna pregrada mora imeti vgrajena dva (2) napajalnika za zagotavljanje podvojenosti, z možnostjo menjave med delovanjem,
7. požarna pregrada mora biti primerna za montažo v strežniško omaro oziroma mora biti priložen ustrezen komplet za montažo v strežniško omaro (angl. rack mountable), višine 1RU in širine 19 palcev.

2.2.3. Podpora vmesnikom na napravi:

- vsaj 4 x SFP (1 Gbps),
- vsaj 4 x SFP+ (10 Gbps),
- vsaj 16 x RJ45 (10Mbps/100Mbps/1Gbps),
- vsaj 1 Gbps (RJ45) port namenjen ločenemu upravljanju naprave.

2.2.4. Funkcionalne lastnosti:

1. aplikacijsko preverjanje in nadziranje prometa se mora vedno izvajati na vsem prometu, ki gre skozi požarno pregrado, ne glede na port ali protokol,
2. požarna pregrada mora podpirati aplikacijsko bazo z več kot 5000 aplikacijami z dinamičnimi filtri na podlagi naslednjih kriterijev: kategorija, podkategorija, vedenjske značilnosti, osnovna tehnologija ali dejavnik tveganja,

3. požarna pregrada mora omogočati zaznavanje in obravnavo neznanih in prej nevidenih groženj na osnovi strojnega učenja in vedenjske analize,
4. požarna pregrada mora omogočati naknadno prepoznavo in klasifikacijo neznanega prometa s posebej napisanimi pravili ali signaturami,
5. požarna pregrada mora omogočati zaščito pred znanimi ranljivosti (IPS), poleg zaščite na osnovi signatur mora omogočati tudi dodatno zaščito pred neznanimi in zero-day napadi v realnem času (inline) z uporabo strojnega učenja in globokega učenja v oblaku proizvajalca naprave,
6. požarna pregrada lahko analizira šifrirani prometa z uporabo TLS finger-printinga tudi brez popolne dešifriranosti vsebine,
7. požarna pregrada mora omogočati blokiranje škodljive programske kode (angl. Antivirus),
8. požarna pregrada mora zagotavljati algoritme strojnega učenja (angl. Machine Learning) za napredno zaščito na sami napravi. S tem mora omogočati hitro, lokalno analizo zero-day groženj in drugih izmikajočih se napadov na osnovi strojnega učenja, pri čemer niso potrebne zunanje povezave. Požarna pregrada mora podpirati analizo Zero-Day zlonamerne programske opreme brez uporabe signatur (za zaznavanje izmikajočega se in neznanega prometa, kot je C2, za zaznavanje orodij, kot sta Cobalt Strike in Empire, proti napadom z vbrizgavanjem ukazov in SQL vbrizgavanjem) in mora podpirati naslednje protokole: HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP in SMB,
9. požarna pregrada mora imeti podporo za IPS podpise za zaznavanje post-kvantnih algoritmov in napadi zmogljivih kvantnih računalnikov (angl. Post Quantum Cyphers),
10. požarna pregrada mora omogočati zaščito pred 0-day napadi; rešitev mora vključevati mehanizme za proaktivno zaznavanje in preprečevanje neznanih groženj (0-day), kot so vedenjska analiza prometa, strojno učenje, detekcija anomalij ter integracija z globalnimi bazami groženj v realnem času,
11. požarna pregrada mora omogočati zaščito pred 0-day napadi s tem da omogoča pošiljanje datotek v analizo v izolirano okolje proizvajalca (angl. Cloud sandbox),
12. v primeru, da proizvajalec požarne pregrade odkrije novo škodljivo kodo in izda ustrezno zaščito, mora požarna pregrada to zaščito prejeti takoj (posodabljanje v realnem času),
13. požarna pregrada mora omogočati prepoznavo morebitnih že okuženih naprav v omrežju (anti-bot, antispyware), poleg zaščite na osnovi signatur mora omogočati tudi dodatno preverjanje sumljivega prometa v realnem času v oblaku proizvajalca naprave,
14. požarna pregrada mora omogočati prepoznavo, spremljanje in blokiranje različnih datotek (izvedljive datoteke, PDF dokumenti MS office dokumenti…) v poljubni smeri (upload ali download),
15. požarna pregrada mora privzeto podpirati tudi skeniranje izvedljivih datotek za macOS in Linux. V tem smislu mora rešitev zagotoviti podrobno analizo vsake analizirane datoteke na več operacijskih sistemih, vključno z informacijami o dejavnosti na ravni naprave in omrežja. Omogočiti mora tudi dostop do izvirne datoteke, vključno s PCAP z dinamično analizo seje, če je datoteka obravnavana kot zlonamerna programska oprema za obratni inženiring, ter podrobno poročilo v PDF-u s statično in dinamično analizo,
16. požarna pregrada mora omogočati vključitev katere koli nove varnostne funkcije, ne da bi to vplivalo na zmogljivost prometa, ki poteka skozi njo. To pomeni, da mora že v osnovi nuditi vsaj kontrolo aplikacij, IPS, protivirusno zaščito, antispyware, sandboxing, blokiranje datotek, URL filtriranje, DNS zaščito in beleženje dogodkov,
17. požarna pregrada mora omogočati možnost zahtevanja URL re-kategorizacije znotraj grafičnega vmesnika požarne pregrade,
18. požarna pregrada mora podpirati varnostne politike z uporabo explicit proxy funkcionalnosti,
19. požarna pregrada mora podpirati možnost ustvarjanja varnostnih politik za preprečevanje kraje poverilnic in preprečevanje uhajanja korporativnih poverilnic na spletne strani tretjih oseb. Pri tem se mora za preverjanje poverilnic uporabiti Bloom filter,
20. požarna pregrada mora dinamično analizirati URL-je v realnem času tudi za sveže generirane URL-je, domene brez zgodovine ter neznane oz. neklasificirane URL-je,

21. požarna pregrada mora dinamično v realnem času analizirati in blokirati dostop do sofisticiranih še nikoli videnih strani lažnega predstavljanja (phishing strani) z uporabo naprednih detekcijskih anti-phishing mehanizmov, ki so osnovani na algoritmih globokega učenja,
22. požarna pregrada mora podpirati zaščito DNS varnosti, kot so: zaznavanje DNS povratnih klicev domen (škodljiva programska oprema in C2 domene, Botnet domene, Fast-flux domene, naključni DGA, dictionary DGA), DNS domen z visokim tveganjem (grayware, novo registrirane domene, parkirane domene, izogibanje proxyjem, dinamični DNS, napovedno zaznavanje, strateško stare domene), napadov na DNS zapise (Domain squatting, dangling DNS, kompromitirana DNS cona, Wildcard DNS, CNAME cloaking), napadov na DNS protokol (DNS Rebinding, NXNS napadi), zaznavanje DNS tuneliranja, ultra-počasno DNS tuneliranje in DNS infiltracije, ter podporo za DNS sinkholing za identifikacijo okuženih naprav v omrežju,
23. Anti-Virus in URL filtriranje podpisov in vsebina morata biti avtorsko delo proizvajalca požarne pregrade (tj. nobena tretja stranka za A/V ali URL filtriranje podpisov),
24. požarna pregrada mora biti sposobna dešifrirati TLS v1.3 seje z uporabo zunanjih Hardware Security Modules (HSM) za shranjevanje zasebnih ključev,
25. požarna pregrada mora omogočati ustvarjanje kopije dešifriranega prometa iz požarne pregrade (angl. Decryption mirroring) in njeno pošiljanje orodjem za zbiranje prometa za forenziko, zgodovinske namene ali preprečevanje izgube podatkov (DLP),
26. požarna pregrada mora podpirati IPS, zaščito pred zlonamerno programsko opremo, filtriranje vsebine in URL filtriranje v enem samem varnostnem pravilu,
27. požarna pregrada mora omogočati dešifriranje SSL/HTTPS in SSH prometa,
28. SSL inspekcija mora biti sposobna v celoti izpolnjevati TLS 1.2 visoke / srednje šifrirne algoritme in ne sme prekiniti pogajanja o TLS 1.3,
29. požarna pregrada mora omogočati spremljanje in uporabo zunanjih dinamičnih seznamov IP naslovov, domen in URL naslovov (integracija z obstoječimi sistemi za zaznavo anomalij v omrežju),
30. požarna pregrada mora omogočati filtriranje spletnih strani na osnovi kategorij ali specifičnih URL naslovov. Administrator poleg tega lahko ustvari in uporablja lastne kategorije in specifične URL naslove v pravilih, ne da bi imel pri tem kakršnekoli omejitve,
31. požarna pregrada mora omogočati samodejno odkrivanje in identifikacija vseh naprav v omrežju (IT, IoT, OT, IoMT, BYOD) brez uporabe agentov,
32. požarna pregrada mora pripisati naslednje lastnosti napravam: tip, proizvajalec, model, operacijski sistem in raven tveganja,
33. požarna pregrada mora dinamično uveljavljati Zero-Trust varnostnih politik glede na kontekst in tveganje naprave,
34. požarna pregrada mora imeti integrirano vidljivost, ocenjevanje tveganj in prioritetna obravnava ranljivosti prepoznanih naprav v omrežju,
35. požarna pregrada lahko agregira SD-WAN povezave oddaljenih lokacij (Hub), ter omogoča aplikacijsko zavedno usmerjanje prometa glede na zakasnitev, izgubo paketov in jitter,
36. požarna pregrada lahko samodejno preusmerjanje prometa brez prekinitve seje (sub-second failover),
37. požarna pregrada mora omogočati hiter vpogled v promet preko požarne pregrade za obdobje zadnjih nekaj ur ali dni, analiziran glede na aplikacijo, izvorni IP naslov ali ciljni IP naslov,
38. požarna pregrada mora omogočati avtomatično izdelavo in hranjenje obdobnih poročil o aplikacijah, prometu in varnostnih dogodkih,
39. požarna pregrada mora omogočati izdelavo lastnih obdobnih poročil glede na poljubne kriterije ali filtre,
40. požarna pregrada mora omogočati izvoz poročil in pošiljanje preko e-pošte,
41. požarna pregrada mora omogočati zaznavo uporabljenih in ne uporabljenih pravil zaradi optimizacije delovanja,

42. požarna pregrada mora omogočati beleženje vseh aplikacij, ki so bile dovoljene po posameznem pravilu (za prehod v aplikacijsko politiko), ter količino prometa za posamezno aplikacijo dovoljenega po tem pravilu,
43. požarna pregrada mora omogočati integracijo s poljubnim LDAP strežnikom za pridobivanje informacij o uporabnikih in uporabniških skupinah,
44. požarna pregrada mora omogočati prepoznavo uporabnikov preko portalov za identifikacijo (angl. Captive portal),
45. požarna pregrada mora omogočati prepoznavo uporabnikov iz drugih sistemov na podlagi syslog sporočil,
46. požarna pregrada mora omogočati pisanje varnostne politike glede na uporabnike in uporabniške skupine,
47. požarna pregrada mora omogočati vpeljavo dodatnega overjanja tudi z uporabo MFA za dostop do najbolj kritičnih sistemov oziroma strežnikov,
48. požarna pregrada mora omogočati izvoz logov preko syslog formatov BSD, IETF ali poljubno definirane oblike (za integracijo s SIEM in ostalimi sistemi),
49. požarna pregrada mora omogočati natančno filtriranje logov pri izvozu preko syslog formata glede na vrsto loga, resnost dogodka, tip dogodka, kategorijo dogodka, pravilo (za integracijo s SIEM in ostalimi sistemi),
50. požarna pregrada mora omogočati preprost pregled vseh dogodkov v realnem času z možnostjo filtriranja prometa vsaj po naslednjih parametrih (izvor prometa, cilj prometa, protokol, ciljni port, izvorni port, uporabnik, namenski program, spletna kategorija),
51. konfiguriranje FW v polni funkcionalnosti, vpogled in analiziranje logov mora biti dostopno lokalno na požarni pregradi, brez potrebe po dodatnih napravah, programski opremi ali licencah,
52. uporabniški vmesnik mora biti grafičen (GUI), dostop in upravljanje preko tega vmesnika mora biti možno brez uporabe namenskih aplikacij, ampak s splošnimi klienti (HTTP/HTTPS – poljuben brskalnik),
53. omogočati mora grafično in objektno orientirano pisanje varnostnih pravil v prejšnji točki opisanemu grafičnem vmesniku (združevanje objektov v skupine, negiranje polj, uporaba več objektov kot vir ali cilj prometa znotraj enega pravila),
54. požarna pregrada mora zagotavljati preglednost ter zmožnost identifikacije in omejevanja aplikacij, ne glede na port, protokol, izmikajoče se tehnike ali šifriranje (TLS/SSL) ali uporabo nestandardnih portov, znotraj enega samega varnostnega pravila,
55. konfiguracija vseh funkcionalnosti mora biti mogoča preko obeh vmesnikov: CLI in GUI,
56. požarna pregrada mora omogočati overjanje uporabnikov tudi preko oblačnih ponudnikov (identitiy provider - IdP) preko SAML 2.0 protokola,
57. požarna pregrada mora omogočati pridobivanje podatkov o uporabnikih tudi iz oblačnih ponudnikov (identitiy provider - IdP) za zagotavljanje ZTNA v vseh okoljih,
58. proizvajalec požarne pregrade mora zagotavljati konstanto spremljanje stanja požarne pregrade glede zasedenosti virov, kritičnih dogodkov ter skladnosti konfiguracije s priporočili dobre prakse (AIOps),
59. požarna pregrada mora podpirati VPN za oddaljeni dostop (preko SSL, IPsec, brez odjemalca (ang.clientless)). Poleg tega mora omogočati preprečevanje mobilnih groženj (mobile threat prevention) in koristenje politik na podlagi aplikacij, uporabnikov, vsebine, naprave in stanja naprave,
60. požarna pregrada mora podpirati avtomatski povratek (ang. fallback) na SSL VPN iz IPSec VPN,
61. požarna pregrada mora podpirati VPN povezave iz naslednjih platform: Microsoft Windows in Apple macOS,
62. požarna pregrada mora podpirati horizontalno skaliranje števila VPN uporabnikov v primeru, da je to potrebno, z uporabo dodatnih NGFW naprav v konfiguraciji brez visoke razpoložljivosti (tj. samostojno),

63. naprava mora omogočati dobro dokumentiran in varen programabilni spletni vmesnik (API) za upravljanje naprave preko API klicev z namenom integracije z naročnikovimi obstoječimi ali bodočimi sistemi za varnostno orkestracijo in samodejno kibernetsko obrambo,
64. naprava mora omogočati uporabo dinamičnih skupin objektov in urejanje članstva v dinamičnih skupinah brez ponovne instalacije (install/deploy/commit) politike naprave,
65. lokalni grafični uporabniški vmesnik (GUI) požarne pregrade in/ali opcijska zunanja centralna upravljalna platforma morata ponujati možnost pregleda razpoložljivih različic programske opreme ter možnost prenosa in aktivacije programskih verzij znotraj njunih vmesnikov,
66. lokalni GUI mora podpirati neposreden prenos in aktivacijo programskih verzij brez odvisnosti od zunanjih orodij ali centralne upravljalne platforme,
67. lokalni grafični vmesnik (GUI) mora natančno odražati delujočo konfiguracijo požarne pregrade, ne glede na to, ali je bila prvotno posredovana s centralne upravljalne platforme ali konfigurirana lokalno,
68. požarna pregrada mora podpirati označevanje in prekategorizacijo QoS na podlagi izvornega/ciljnega IP-ja, porta, protokola in aplikacije.

2.2.5. Zahtevani optični moduli in povezovalni kabli

Naročnik potrebuje šestnajst (16) kosov 10G SFP+ optičnih modulov kompatibilnih s ponujeno opremo ter osem (8) pripadajočih povezovalnih optičnih kablov dolžine 5 metrov. Navedeno se lahko nadomesti z osem (8) 10G SFP+ AOC pripravljenih povezovalnih kablov dolžine 5 metrov.

2.2.6. Zahtevana programska oprema, naročnine in licence:

- programska oprema mora zagotavljati vse zgoraj zahtevane funkcionalnosti,
- v primeru, da je za delovanje zgoraj naštetih funkcionalnosti potreba ustrezna licenca ali naročnina, mora biti vključena za ves čas trajanja pogodbe;
- aktivacija/e, naročnina/e, licenčnina/e in vzdrževanje za vse zgoraj navedene zahteve/funkcionalnosti morajo biti zajete v ponudbeni ceni in za naročnika ne smejo predstavljati dodatnih stroškov.

2.3. Lokacija in obseg izvajanja storitev

Storitve se izvajajo na dveh geografsko ločenih lokacijah (v Ljubljani in Kopru). Na obeh lokacijah naročnik pričakuje izvedbo naslednjih storitev:

1. vzpostavitev HA para v telekomunikacijsko omarico, povezava v obstoječe omrežje, povezava HA in MGMT vmesnikov,
2. osnovna konfiguracija (HA, Management, licenciranje, posodobitev),
3. priprava izvedbenega načrta migracije,
4. čiščenje neuporabljenih objektov in pravil, varnostna optimizacija varnostnih pravil in pravil NAT,
5. izvoz obstoječe konfiguracije in uvoz na novo opremo,
6. priprava VPN infrastrukture, uvedba centraliziranega RAVPN dostopa, integracija z aktivnim imenikom,
7. implementacija multifaktorske avtentikacije za VPN dostop,
8. konfiguracija varnostnih pravil glede na identitete uporabnikov,
9. vključevanje naprednih NGFW funkcionalnosti na pravilih (DNS Security, AS, IPS,...),
10. selitev URL politike iz forward proxy na NGFW,
11. prestavitev BGP peering iz obstoječih usmerjevalnikov na NGFW,
12. optimizacija varnostnih pravil – izbris neuporabljenih pravil, združevanje pravil, migracija pravil.

2.4. Rok za dobavo in namestitev opreme

Rok za dobavo, namestitev in konfiguracijo ter primopredajo obeh požarnih pregrad (vključno s tehnično dokumentacijo) in izvedbo vseh storitev, ki so predmet javnega naročila, je 90 dni od dneva podpisa pogodbe.

2.5. Garancijski pogoji

Garancija za vso dobavljeno komunikacijsko strojno opremo je 36 mesecev in je všteta v ceno.

Za pripadajočo programsko opremo veljajo garancijski in licenčni pogoji, kot jih proizvajalec te opreme nudi za posamezne programske proizvode.

Garancijski rok začne teči od dneva podpisa dobavnice. Če je bila oprema v garancijskem roku zamenjana ali bistveno popravljena, začne garancijski rok znova in je prodajalec dolžan izdati nov garancijski list.

Dobava in namestitev rezervnih delov ter vsi drugi stroški v zvezi s popravilom v času garancijskega roka bremenijo dobavitelja / izvajalca.

Dobavitelj / izvajalec ne jamči v naslednjih primerih:
- če naročnik z opremo ni ravnal po navodilih za uporabo, ki so priložena izdelkom,
- če je v izdelek posegla nepooblaščena oseba,
- če naročnik nestrokovno in malomarno ravna z izdelkom.

Garancija ne pokriva:
- okvar, povzročenih pri transportu po izročitvi blaga,
- mehanskih okvar, ki jih povzroči naročnik,
- okvar, povzročenih zaradi nihanja električne napetosti ali udara strele in prenapetostnega udara,
- okvar, povzročenih zaradi neustrezne temperature ali vlage,
- okvar, povzročenih zaradi višje sile.

2.6. Režim garancijskega vzdrževanja opreme

Naročniku mora biti zagotovljena možnost, da lahko prijavi napako 24 ur in 7 dni v tednu.

V primeru nepravilnega delovanja programske opreme mora izvajalec naročniku nuditi tehnično pomoč in obvestiti proizvajalčev center za tehnično pomoč o zaznani napaki.

Ko proizvajalec dobavi novo različico programske opreme, mora izvajalec v dogovoru z naročnikom namestiti novo programsko opremo.

V primeru prijave okvare do 12. ure mora izvajalec okvaro na opremi odpraviti v istem delovnem dnevu, v primeru prijave okvare po 12. uri mora izvajalec okvaro na opremi odpraviti najpozneje naslednji delovni dan.

Vzdrževanje mora vključevati tudi:
1. vodenje vseh postopkov prijave, obravnave in odprave napak pri proizvajalcu,
2. neposreden (7x24x365) dostop do proizvajalčevega centra za tehnično pomoč,

3. dostop do novih verzij programske opreme,
4. pravico do vseh novih verzij programske opreme (v okviru funkcionalnosti), kot jih dobavlja proizvajalec opreme,
5. obveščanje naročnika o novih verzijah in spremembah v njih
6. vodenje dokumentacije vzdrževalnih posegov na opremi naročnika tako, da je naročniku zagotovljena možnost vpogleda v dokumentacijo preko interneta za čas trajanja pogodbe,
7. obveščanje naročnika o varnostnih problemih z obstoječimi verzijami programske opreme in takojšnja izvedba akcij v dogovoru z naročnikom, če obstaja varnostna ogroženost na opremi, ki jo ima naročnik;
8. dostop do tehnoloških informacij proizvajalca opreme v času trajanja te pogodbe.

Izvajalec mora ob sklenitvi pogodbe naročniku posredovati telefonsko število in elektronski naslov, na katerem je dosegljiv nadzornik sistema.

Komunikacija s klicnim centrom se mora izvajati v slovenskem jeziku; tehnično osebje, ki komunicira z naročnikom, mora tekoče govoriti slovensko.

Naročnik lahko kadarkoli med izvajanjem pogodbe preveri nivo zagotavljanja storitve.

3. Vzorec pogodbe

Republika Slovenija, Ministrstvo za finance, Uprava Republike Slovenije za javna plačila, Dunajska cesta 48, 1000 Ljubljana, davčna številka 10641424, matična številka 1572814000, ki jo zastopa Urška Kos, generalna direktorica (v nadaljnjem besedilu: **UJP ali naročnik**)

in

_____, davčna številka _____, matična številka _____, ki ga zastopa _____
(v nadaljnjem besedilu: **prodajalec** ali **izvajalec**)

skleneta naslednjo

POGODBO
o dobavi, namestitvi, konfiguraciji in garancijskem vzdrževanju
požarnih pregrad v komunikacijskem omrežju
številka _____

1. SPLOŠNO

1. člen

Pogodbeni stranki uvodoma ugotavljata:

- da je naročnik izvedel postopek oddaje javnega naročila *»Dobava, namestitev, konfiguracija in garancijsko vzdrževanje dveh (2) kompletov požarnih pregrad v komunikacijskem omrežju«,* z oznako 4/2026-JNMV-PP, na podlagi določb 47. člena Zakona o javnem naročanju (Uradni list RS, št. 91/15, 14/18, 121/21, 10/22, 74/22 – odl. US, 100/22 – ZNUZSZS, 28/23, 88/23 – ZOPNN-F in 83/25 - ZOUL; v nadaljnjem besedilu: ZJN-3) in obvestila o javnem naročilu, objavljenega na portalu javnih naročil (številka objave _____z dne _____), ter v skladu z dokumentacijo v zvezi z oddajo javnega naročila, številka 430-86/2026-__ z dne __11. 2026 (v nadaljnjem besedilu: razpisna dokumentacija), ki je bila objavljena prek portala javnih naročil);
- da je bil izvajalec izbran kot najugodnejši ponudnik na podlagi odločitve o oddaji javnega naročila, št. _____ z dne _____, ki je postala pravnomočna dne _____.

2. PREDMET POGODBE

2.1. Opis blaga in storitev

2. člen

(1) S to pogodbo se izvajalec zavezuje, da bo naročniku dobavil dva (2) kompleta požarnih pregrad v komunikacijskem omrežju s pripadajočo opremo (v nadaljevanju: oprema) ter opravil storitve po naslednji specifikaciji:

Zap. št.	Predmet ponudbe	Ponujeni proizvajalec, tip/model oziroma oznaka	Enota mere	Količina	Cena na enoto brez DDV (EUR)	Skupna vrednost brez DDV (EUR)
1.1	Požarna pregrada Palo Alto Networks PA-560 ali enakovredna, skladna s tehničnimi zahtevami naročnika		kos	2		
1.2	Naročnina Precision AI Network Security Subscription Bundle za PA-560, ki vključuje Advanced Threat Prevention in Advanced URL Filtering, ali enakovredna naročnina za obdobje treh (3) let		kos	2		
1.3	Napajalnik 150 W za PA-560 ali enakovreden za zagotavljanje redundantnega napajanja		kos	2		
1.4	Komplet 10G SFP+ modulov in povezovalnih optičnih kablov dolžine 5m *(1 komplet = 2xSFP+ modul in 1x povezovalni kabel)*		komplet	8		
1.5	Storitve dobave, namestitve, konfiguracije, migracije, testiranja in primopredaje rešitve		komplet	1		
1.6	Vzdrževanje, tehnična podpora v režimu 24x7 in dostop do posodobitev za celotno rešitev za obdobje treh (3) let		komplet /mesec	36 mesecev	*0,00	*0,00
Skupna ponudbena vrednost brez DDV (EUR)						
DDV (EUR)						
Skupna ponudbena vrednost z DDV (EUR)						

(2) *Garancijsko vzdrževanje je brezplačno oziroma všteto v kupnino/ceno opreme.

(3) DDV se obračuna po veljavni davčni stopnji.

(4) V ceno brez DDV so vključeni naslednji stroški:
- kupnina za dva (2) kompleta požarnih pregrad v komunikacijskem omrežju (vključno s pripadajočo opremo),
- kupnina za licence,
- storitve, povezane z namestitvijo in konfiguracijo opreme,
- vzdrževanje strojne opreme,
- cena delovne ure serviserja, pripravljenost, potni stroški, čas servisiranja itd.,

- zagotavljanje odzivnega časa in popravila v zahtevanem režimu vzdrževanja,
- stroški rezervnih delov in nadomestne računalniške opreme,
- stroški potrošnega materiala in medijev potrebnih za izvedbo vzdrževanja,
- stroški skladiščenja priporočenih rezervnih delov in opreme, ki omogoča zamenjavo v zahtevanem režimu,
- tehnična podpora za licenčno programsko opremo,
- stroški, povezani z nadgradnjo in novimi verzijami programske opreme,
- sistemsko konfiguriranje,
- pomoč po telefonu,
- usposabljanje uporabnikov računalniške opreme, zaposlenih pri naročniku,
- zagotavljanje uporabniške dokumentacije,
- zagotavljanje garancij za rezervne dele, opremo in opravljene storitve,
- stroški, povezani z zagotavljanjem ustreznih finančnih zavarovanj za dobro izvedbo pogodbenih obveznosti in odpravo napak v garancijskem roku,
- drugi stroški, ki se neposredno ali posredno nanašajo na dobavo, namestitev, konfiguracijo in vzdrževanje opreme.

2.2. Splošne zahteve za strojno opremo

3. člen

Oprema mora omogočati oddaljeni dostop za 150 uporabnikov naročnika (RAVPN).

Ponujena oprema mora biti funkcionalno in protokolno združljiva z obstoječim komunikacijskim omrežjem naročnika, tehnično preverjena ter mora zagotavljati zanesljivo delovanje v obstoječem sistemu oziroma omrežju.

Oprema mora biti skladna z zahtevano konfiguracijo, namenjena slovenskemu trgu ter opremljena z vsemi potrebnimi veljavnimi atesti in dovoljenji za uporabo v Republiki Sloveniji. Omogočati mora uporabo in vzdrževanje v Sloveniji brez dodatnih prilagoditev ali sprememb.

Vsa strojna oprema mora biti nova in proizvedena v letu 2026.

Izvajalec mora biti pooblaščen serviser ponujene opreme ter mora zagotavljati rezervne dele za vso ponujeno opremo v zahtevani konfiguraciji najmanj pet (5) let od dneva primopredaje opreme.

2.3. Tehnične zahteve in lastnosti obeh požarnih pregrad

4. člen

Navedene lastnosti in zmogljivosti veljajo za dve požarni pregradi:

2.3.1. Splošne lastnosti:

1. požarna pregrada mora omogočati aplikacijsko pregledovanje in nadziranje prometa (angl. NGFW požarna pregrada),
2. požarna pregrada mora imeti zasnovo primerno za okolja z visoko zanesljivostjo (active/passive HA),
3. požarna pregrada mora biti namenska naprava (virtualna naprava ni sprejemljiva),
4. proizvajalec požarne pregrade se mora nahajati v četrtem (leader) kvadrantu Gartner poročil za Next-Generation požarne pregrade vsaj zadnjih 5 let,
5. postavitev požarne pregrade mora omogočati naslednje scenarije:
   - transparentni prehod za prestrezanje (Virtual Wire),
   - L3 način (požarna pregrada je privzeti prehod napravam v omrežju),

- o zajem kopije prometa za analizo (tap),
- o L2 način,

6. požarna pregrada mora imeti fizično ločeno upravljalno ravnino (angl. Management plane), ki skrbi za grafični vmesnik in konfiguracijo, ter podatkovno ravnino (angl. Data plane), ki obravnava promet, ki poteka skozi požarno pregrado. Poleg tega mora imeti požarna pregrada najmanj 2 CPU jedri, namenjeni izključno upravljalni ravnini,
7. požarna pregrada mora imeti fizično ločen upravljalni vmesnik (out-of-band management), ki omogoča popolno izolacijo upravljanja od produkcijskega prometa.

2.3.2. Tehnične zmogljivosti:

1. požarna pregrada mora biti strojna, namenska naprava, optimizirana z ustreznimi pospeševalnimi komponentami (npr. ASIC, FPGA), tako da vse NGFW storitve izvaja pospešeno na namenski strojni opremi; poizvedbe na upravljalni ravnini pri tem ne smejo vplivati na pretočni oziroma podatkovni del,
2. požarna pregrada mora omogočati vsaj 8,5 Gbps prepustnosti pri aplikacijskem pregledovanju in nadzoru vsega prometa,
3. požarna pregrada mora omogočati vsaj 6 Gbps prepustnosti pri aplikacijskem pregledovanju in nadzoru vsega prometa ter pri vključenih vseh varnostnih preverjanjih prometa (angl. Threat Prevention Throughput). Navedena zahteva se ne nanaša zgolj na prepustnost pri varnostnih preverjanjih, ki so predmet tega naročila, temveč mora biti zagotovljena tudi ob morebitnem kasnejšem dodajanju novih varnostnih preverjanj,
4. požarna pregrada mora omogočati vsaj 5,5 Gbps prepustnosti pri prometu IPSec VPN, najmanj 598.000 sočasnih sej, najmanj 100.000 novih sej na sekundo ter najmanj 10 virtualnih usmerjevalnikov (npr. VRF),
5. požarna pregrada mora podpirati virtualizacijo oziroma razdelitev na najmanj pet (5) virtualnih razdelkov z neodvisnimi vmesniki in politikami ter že vključevati možnost uporabe vsaj enega (1) virtualnega razdelka (virtualni sistemi, konteksti),
6. požarna pregrada mora imeti vgrajena dva (2) napajalnika za zagotavljanje podvojenosti, z možnostjo menjave med delovanjem,
7. požarna pregrada mora biti primerna za montažo v strežniško omaro oziroma mora biti priložen ustrezen komplet za montažo v strežniško omaro (angl. rack mountable), višine 1RU in širine 19 palcev.

2.3.3. Podpora vmesnikom na napravi:

- vsaj 4 x SFP (1 Gbps),
- vsaj 4 x SFP+ (10 Gbps),
- vsaj 16 x RJ45 (10Mbps/100Mbps/1Gbps),
- vsaj 1 Gbps (RJ45) port namenjen ločenemu upravljanju naprave.

2.3.4. Funkcionalne lastnosti:

1. aplikacijsko preverjanje in nadziranje prometa se mora vedno izvajati na vsem prometu, ki gre skozi požarno pregrado, ne glede na port ali protokol,
2. požarna pregrada mora podpirati aplikacijsko bazo z več kot 5000 aplikacijami z dinamičnimi filtri na podlagi naslednjih kriterijev: kategorija, podkategorija, vedenjske značilnosti, osnovna tehnologija ali dejavnik tveganja,
3. požarna pregrada mora omogočati zaznavanje in obravnavo neznanih in prej nevidenih groženj na osnovi strojnega učenja in vedenjske analize,
4. požarna pregrada mora omogočati naknadno prepoznavo in klasifikacijo neznanega prometa s posebej napisanimi pravili ali signaturami,
5. požarna pregrada mora omogočati zaščito pred znanimi ranljivosti (IPS), poleg zaščite na osnovi signatur mora omogočati tudi dodatno zaščito pred neznanimi in zero-day napadi v

realnem času (inline) z uporabo strojnega učenja in globokega učenja v oblaku proizvajalca naprave,

6. požarna pregrada lahko analizira šifrirani prometa z uporabo TLS finger-printinga tudi brez popolne dešifriranosti vsebine,
7. požarna pregrada mora omogočati blokiranje škodljive programske kode (angl. Antivirus),
8. požarna pregrada mora zagotavljati algoritme strojnega učenja (angl. Machine Learning) za napredno zaščito na sami napravi. S tem mora omogočati hitro, lokalno analizo zero-day groženj in drugih izmikajočih se napadov na osnovi strojnega učenja, pri čemer niso potrebne zunanje povezave. Požarna pregrada mora podpirati analizo Zero-Day zlonamerne programske opreme brez uporabe signatur (za zaznavanje izmikajočega se in neznanega prometa, kot je C2, za zaznavanje orodij, kot sta Cobalt Strike in Empire, proti napadom z vbrizgavanjem ukazov in SQL vbrizgavanjem) in mora podpirati naslednje protokole: HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP in SMB,
9. požarna pregrada mora imeti podporo za IPS podpise za zaznavanje post-kvantnih algoritmov in napadi zmogljivih kvantnih računalnikov (angl. Post Quantum Cyphers),
10. požarna pregrada mora omogočati zaščito pred 0-day napadi; rešitev mora vključevati mehanizme za proaktivno zaznavanje in preprečevanje neznanih groženj (0-day), kot so vedenjska analiza prometa, strojno učenje, detekcija anomalij ter integracija z globalnimi bazami groženj v realnem času,
11. požarna pregrada mora omogočati zaščito pred 0-day napadi s tem da omogoča pošiljanje datotek v analizo v izolirano okolje proizvajalca (angl. Cloud sandbox),
12. v primeru, da proizvajalec požarne pregrade odkrije novo škodljivo kodo in izda ustrezno zaščito, mora požarna pregrada to zaščito prejeti takoj (posodabljanje v realnem času),
13. požarna pregrada mora omogočati prepoznavo morebitnih že okuženih naprav v omrežju (anti-bot, antispyware), poleg zaščite na osnovi signatur mora omogočati tudi dodatno preverjanje sumljivega prometa v realnem času v oblaku proizvajalca naprave,
14. požarna pregrada mora omogočati prepoznavo, spremljanje in blokiranje različnih datotek (izvedljive datoteke, PDF dokumenti MS office dokumenti…) v poljubni smeri (upload ali download),
15. požarna pregrada mora privzeto podpirati tudi skeniranje izvedljivih datotek za macOS in Linux. V tem smislu mora rešitev zagotoviti podrobno analizo vsake analizirane datoteke na več operacijskih sistemih, vključno z informacijami o dejavnosti na ravni naprave in omrežja. Omogočiti mora tudi dostop do izvirne datoteke, vključno s PCAP z dinamično analizo seje, če je datoteka obravnavana kot zlonamerna programska oprema za obratni inženiring, ter podrobno poročilo v PDF-u s statično in dinamično analizo,
16. požarna pregrada mora omogočati vključitev katere koli nove varnostne funkcije, ne da bi to vplivalo na zmogljivost prometa, ki poteka skozi njo. To pomeni, da mora že v osnovi nuditi vsaj kontrolo aplikacij, IPS, protivirusno zaščito, antispyware, sandboxing, blokiranje datotek, URL filtriranje, DNS zaščito in beleženje dogodkov,
17. požarna pregrada mora omogočati možnost zahtevanja URL re-kategorizacije znotraj grafičnega vmesnika požarne pregrade,
18. požarna pregrada mora podpirati varnostne politike z uporabo explicit proxy funkcionalnosti,
19. požarna pregrada mora podpirati možnost ustvarjanja varnostnih politik za preprečevanje kraje poverilnic in preprečevanje uhajanja korporativnih poverilnic na spletne strani tretjih oseb. Pri tem se mora za preverjanje poverilnic uporabiti Bloom filter,
20. požarna pregrada mora dinamično analizirati URL-je v realnem času tudi za sveže generirane URL-je, domene brez zgodovine ter neznane oz. neklasificirane URL-je,
21. požarna pregrada mora dinamično v realnem času analizirati in blokirati dostop do sofisticiranih še nikoli videnih strani lažnega predstavljanja (phishing strani) z uporabo naprednih detekcijskih anti-phishing mehanizmov, ki so osnovani na algoritmih globokega učenja,
22. požarna pregrada mora podpirati zaščito DNS varnosti, kot so: zaznavanje DNS povratnih klicev domen (škodljiva programska oprema in C2 domene, Botnet domene, Fast-flux

domene, naključni DGA, dictionary DGA), DNS domen z visokim tveganjem (grayware, novo registrirane domene, parkirane domene, izogibanje proxyjem, dinamični DNS, napovedno zaznavanje, strateško stare domene), napadov na DNS zapise (Domain squatting, dangling DNS, kompromitirana DNS cona, Wildcard DNS, CNAME cloaking), napadov na DNS protokol (DNS Rebinding, NXNS napadi), zaznavanje DNS tuneliranja, ultra-počasno DNS tuneliranje in DNS infiltracije, ter podporo za DNS sinkholing za identifikacijo okuženih naprav v omrežju,

23. Anti-Virus in URL filtriranje podpisov in vsebina morata biti avtorsko delo proizvajalca požarne pregrade (tj. nobena tretja stranka za A/V ali URL filtriranje podpisov),
24. požarna pregrada mora biti sposobna dešifrirati TLS v1.3 seje z uporabo zunanjih Hardware Security Modules (HSM) za shranjevanje zasebnih ključev,
25. požarna pregrada mora omogočati ustvarjanje kopije dešifriranega prometa iz požarne pregrade (angl. Decryption mirroring) in njeno pošiljanje orodjem za zbiranje prometa za forenziko, zgodovinske namene ali preprečevanje izgube podatkov (DLP),
26. požarna pregrada mora podpirati IPS, zaščito pred zlonamerno programsko opremo, filtriranje vsebine in URL filtriranje v enem samem varnostnem pravilu,
27. požarna pregrada mora omogočati dešifriranje SSL/HTTPS in SSH prometa,
28. SSL inspekcija mora biti sposobna v celoti izpolnjevati TLS 1.2 visoke / srednje šifrirne algoritme in ne sme prekiniti pogajanja o TLS 1.3,
29. požarna pregrada mora omogočati spremljanje in uporabo zunanjih dinamičnih seznamov IP naslovov, domen in URL naslovov (integracija z obstoječimi sistemi za zaznavo anomalij v omrežju),
30. požarna pregrada mora omogočati filtriranje spletnih strani na osnovi kategorij ali specifičnih URL naslovov. Administrator poleg tega lahko ustvari in uporablja lastne kategorije in specifične URL naslove v pravilih, ne da bi imel pri tem kakršnekoli omejitve,
31. požarna pregrada mora omogočati samodejno odkrivanje in identifikacija vseh naprav v omrežju (IT, IoT, OT, IoMT, BYOD) brez uporabe agentov,
32. požarna pregrada mora pripisati naslednje lastnosti napravam: tip, proizvajalec, model, operacijski sistem in raven tveganja,
33. požarna pregrada mora dinamično uveljavljati Zero-Trust varnostnih politik glede na kontekst in tveganje naprave,
34. požarna pregrada mora imeti integrirano vidljivost, ocenjevanje tveganj in prioritetna obravnava ranljivosti prepoznanih naprav v omrežju,
35. požarna pregrada lahko agregira SD-WAN povezave oddaljenih lokacij (Hub), ter omogoča aplikacijsko zavedno usmerjanje prometa glede na zakasnitev, izgubo paketov in jitter,
36. požarna pregrada lahko samodejno preusmerjanje prometa brez prekinitve seje (sub-second failover),
37. požarna pregrada mora omogočati hiter vpogled v promet preko požarne pregrade za obdobje zadnjih nekaj ur ali dni, analiziran glede na aplikacijo, izvorni IP naslov ali ciljni IP naslov,
38. požarna pregrada mora omogočati avtomatično izdelavo in hranjenje obdobnih poročil o aplikacijah, prometu in varnostnih dogodkih,
39. požarna pregrada mora omogočati izdelavo lastnih obdobnih poročil glede na poljubne kriterije ali filtre,
40. požarna pregrada mora omogočati izvoz poročil in pošiljanje preko e-pošte,
41. požarna pregrada mora omogočati zaznavo uporabljenih in ne uporabljenih pravil zaradi optimizacije delovanja,
42. požarna pregrada mora omogočati beleženje vseh aplikacij, ki so bile dovoljene po posameznem pravilu (za prehod v aplikacijsko politiko), ter količino prometa za posamezno aplikacijo dovoljenega po tem pravilu,
43. požarna pregrada mora omogočati integracijo s poljubnim LDAP strežnikom za pridobivanje informacij o uporabnikih in uporabniških skupinah,

44. požarna pregrada mora omogočati prepoznavo uporabnikov preko portalov za identifikacijo (angl. Captive portal),
45. požarna pregrada mora omogočati prepoznavo uporabnikov iz drugih sistemov na podlagi syslog sporočil,
46. požarna pregrada mora omogočati pisanje varnostne politike glede na uporabnike in uporabniške skupine,
47. požarna pregrada mora omogočati vpeljavo dodatnega overjanja tudi z uporabo MFA za dostop do najbolj kritičnih sistemov oziroma strežnikov,
48. požarna pregrada mora omogočati izvoz logov preko syslog formatov BSD, IETF ali poljubno definirane oblike (za integracijo s SIEM in ostalimi sistemi),
49. požarna pregrada mora omogočati natančno filtriranje logov pri izvozu preko syslog formata glede na vrsto loga, resnost dogodka, tip dogodka, kategorijo dogodka, pravilo (za integracijo s SIEM in ostalimi sistemi),
50. požarna pregrada mora omogočati preprost pregled vseh dogodkov v realnem času z možnostjo filtriranja prometa vsaj po naslednjih parametrih (izvor prometa, cilj prometa, protokol, ciljni port, izvorni port, uporabnik, namenski program, spletna kategorija),
51. konfiguriranje FW v polni funkcionalnosti, vpogled in analiziranje logov mora biti dostopno lokalno na požarni pregradi, brez potrebe po dodatnih napravah, programski opremi ali licencah,
52. uporabniški vmesnik mora biti grafičen (GUI), dostop in upravljanje preko tega vmesnika mora biti možno brez uporabe namenskih aplikacij, ampak s splošnimi klienti (HTTP/HTTPS – poljuben brskalnik),
53. omogočati mora grafično in objektno orientirano pisanje varnostnih pravil v prejšnji točki opisanemu grafičnem vmesniku (združevanje objektov v skupine, negiranje polj, uporaba več objektov kot vir ali cilj prometa znotraj enega pravila),
54. požarna pregrada mora zagotavljati preglednost ter zmožnost identifikacije in omejevanja aplikacij, ne glede na port, protokol, izmikajoče se tehnike ali šifriranje (TLS/SSL) ali uporabo nestandardnih portov, znotraj enega samega varnostnega pravila,
55. konfiguracija vseh funkcionalnosti mora biti mogoča preko obeh vmesnikov: CLI in GUI,
56. požarna pregrada mora omogočati overjanje uporabnikov tudi preko oblačnih ponudnikov (identitiy provider - IdP) preko SAML 2.0 protokola,
57. požarna pregrada mora omogočati pridobivanje podatkov o uporabnikih tudi iz oblačnih ponudnikov (identitiy provider - IdP) za zagotavljanje ZTNA v vseh okoljih,
58. proizvajalec požarne pregrade mora zagotavljati konstanto spremljanje stanja požarne pregrade glede zasedenosti virov, kritičnih dogodkov ter skladnosti konfiguracije s priporočili dobre prakse (AIOps),
59. požarna pregrada mora podpirati VPN za oddaljeni dostop (preko SSL, IPsec, brez odjemalca (ang.clientless)). Poleg tega mora omogočati preprečevanje mobilnih groženj (mobile threat prevention) in koristenje politik na podlagi aplikacij, uporabnikov, vsebine, naprave in stanja naprave,
60. požarna pregrada mora podpirati avtomatski povratek (ang. fallback) na SSL VPN iz IPSec VPN,
61. požarna pregrada mora podpirati VPN povezave iz naslednjih platform: Microsoft Windows in Apple macOS,
62. požarna pregrada mora podpirati horizontalno skaliranje števila VPN uporabnikov v primeru, da je to potrebno, z uporabo dodatnih NGFW naprav v konfiguraciji brez visoke razpoložljivosti (tj. samostojno),
63. naprava mora omogočati dobro dokumentiran in varen programabilni spletni vmesnik (API) za upravljanje naprave preko API klicev z namenom integracije z naročnikovimi obstoječimi ali bodočimi sistemi za varnostno orkestracijo in samodejno kibernetsko obrambo,
64. naprava mora omogočati uporabo dinamičnih skupin objektov in urejanje članstva v dinamičnih skupinah brez ponovne instalacije (install/deploy/commit) politike naprave,

65. lokalni grafični uporabniški vmesnik (GUI) požarne pregrade in/ali opcijska zunanja centralna upravljalna platforma morata ponujati možnost pregleda razpoložljivih različic programske opreme ter možnost prenosa in aktivacije programskih verzij znotraj njunih vmesnikov,
66. lokalni GUI mora podpirati neposreden prenos in aktivacijo programskih verzij brez odvisnosti od zunanjih orodij ali centralne upravljalne platforme,
67. lokalni grafični vmesnik (GUI) mora natančno odražati delujočo konfiguracijo požarne pregrade, ne glede na to, ali je bila prvotno posredovana s centralne upravljalne platforme ali konfigurirana lokalno,
68. požarna pregrada mora podpirati označevanje in prekategorizacijo QoS na podlagi izvornega/ciljnega IP-ja, porta, protokola in aplikacije.

2.3.5. Zahtevani optični moduli in povezovalni kabli

Naročnik potrebuje šestnajst (16) kosov 10G SFP+ optičnih modulov kompatibilnih s ponujeno opremo ter osem (8) pripadajočih povezovalnih optičnih kablov dolžine 5 metrov. Navedeno se lahko nadomesti z osem (8) 10G SFP+ AOC pripravljenih povezovalnih kablov dolžine 5 metrov.

2.3.6. Zahtevana programska oprema, naročnine in licence:

- programska oprema mora zagotavljati vse zgoraj zahtevane funkcionalnosti,
- v primeru, da je za delovanje zgoraj naštetih funkcionalnosti potreba ustrezna licenca ali naročnina, mora biti vključena za ves čas trajanja pogodbe;
- aktivacija/e, naročnina/e, licenčnina/e in vzdrževanje za vse zgoraj navedene zahteve/funkcionalnosti morajo biti zajete v ponudbeni ceni in za naročnika ne smejo predstavljati dodatnih stroškov.

2.4. Lokacija in obseg izvajanja storitev

5. člen

Dobava opreme se izvaja na dveh geografsko ločenih lokacijah (v Ljubljani in Kopru). Na obeh lokacijah naročnik pričakuje izvedbo naslednjih storitev:

1. vzpostavitev HA para v telekomunikacijsko omarico, povezava v obstoječe omrežje, povezava HA in MGMT vmesnikov,
2. osnovna konfiguracija (HA, Management, licenciranje, posodobitev),
3. priprava izvedbenega načrta migracije,
4. čiščenje neuporabljenih objektov in pravil, varnostna optimizacija varnostnih pravil in pravil NAT,
5. izvoz obstoječe konfiguracije in uvoz na novo opremo,
6. priprava VPN infrastrukture, uvedba centraliziranega RAVPN dostopa, integracija z aktivnim imenikom,
7. implementacija multifaktorske avtentikacije za VPN dostop,
8. konfiguracija varnostnih pravil glede na identitete uporabnikov,
9. vključevanje naprednih NGFW funkcionalnosti na pravilih (DNS Security, AS, IPS,...),
10. selitev URL politike iz forward proxy na NGFW,
11. prestavitev BGP peering iz obstoječih usmerjevalnikov na NGFW,
12. optimizacija varnostnih pravil – izbris neuporabljenih pravil, združevanje pravil, migracija pravil.

6. člen

Izvajalec bo pogodbena dela izvedel samostojno in brez sodelovanja podizvajalcev.

**Opomba UJP: V primeru skupne ponudbe ali ponudbe s podizvajalci si naročnik pridržuje pravico da ta člen dopolni ali doda nov člen, v katerem se podrobneje določijo pravice in obveznosti, vezane na sodelovanje drugih ponudnikov oziroma podizvajalcev, skladno z zahtevami ZJN-3 in razpisne dokumentacije.*

x. člen

Izvajalec bo del javnega naročila izvajal s podizvajalci po naslednji specifikaciji:

Zap. št.	*Naziv, sedež, matična in davčna številka ter transakcijski račun podizvajalca*	*Opis, vrsta in količina pogodbenih del*	*Kraj izvajanja pogodbenih del*	*Ocenjena vrednost pogodbenih del podizvajalca v EUR brez DDV in z DDV*	*Podizvajalec zahteva neposredna plačila (DA/NE)*

x. člen

Izvajalec mora med izvajanjem javnega naročila naročnika obvestiti o morebitnih spremembah informacij podizvajalcev, določenih v drugem odstavku 94. člena ZJN-3, in poslati informacije o novih podizvajalcih, ki jih namerava naknadno vključiti v izvajanje pogodbe, in sicer najkasneje v petih dneh po spremembi. V primeru vključitve novih podizvajalcev bo moral dobavitelj skupaj z obvestilom posredovati tudi podatke in dokumente iz druge, tretje in četrte alineje drugega odstavka 94. člena ZJN-3.

Naročnik bo zavrnil vsakega naknadno nominiranega podizvajalca:

- *če zanj obstajajo razlogi za izključitev, kot so navedeni v razpisni dokumentaciji ter zahteval zamenjavo,*
- *če bi to lahko vplivalo na nemoteno izvajanje ali dokončanje del,*
- *če novi podizvajalec ne izpolnjuje pogojev v zvezi z oddajo javnega naročila.*

xx. člen

Neposredna plačila podizvajalcem so obvezna le podizvajalcem, ki to izrecno zahtevajo v skladu s 94. členom ZJN-3 in so v ta namen k ponudbi izvajalca priložili pisno izjavo/soglasje (obrazec št. ___). V zvezi s pogodbenimi deli podizvajalcev, ki zahtevajo neposredna plačila, izvajalec pooblašča naročnika, da na podlagi potrjenih računov oziroma situacij neposredno plačuje podizvajalcem dela, ki jih bodo ti opravljali po tej pogodbi.

xx. člen

Za podizvajalce, ki zahtevajo neposredna plačila, mora izvajalec računu obvezno priložiti predhodno potrjene račune podizvajalca (-cev), ki je (so) opravljal(i) storitve oziroma dobave blaga po tej pogodbi.

Za tiste nominirane podizvajalce, ki neposrednih plačil ne bodo zahtevali, bo naročnik od glavnega izvajalca zahteval, da mu najpozneje v 60 dneh od plačila končnega računa oziroma situacije pošlje svojo pisno izjavo in pisno izjavo podizvajalca, da je podizvajalec prejel plačilo za izvedena dela. Če izvajalec ne ravna skladno s tem določilom, bo naročnik Državni revizijski komisiji podal predlog za uvedbo postopka o prekršku iz 2. točke prvega odstavka 112. člena ZJN-3.

xx. člen

Izvajalec mora imeti, ob sklenitvi te pogodbe oziroma na dan začetka in v času njenega izvajanja, sklenjene pogodbe s podizvajalci. V primeru morebitne zamenjave podizvajalcev mora izvajalec naročnika o tem pisno obvestiti v petih (5) dneh po spremembi in mu predložiti sklenjene pogodbe z novimi podizvajalci.

xx. člen

V razmerju do naročnika izvajalec v celoti odgovarja za izvedbo vseh storitev, ki so predmet te pogodbe.

Izvajalec se zavezuje, da bo opravljal nadzor nad podizvajalci.

xx. člen

Če naročnik ugotovi, da dela izvaja podizvajalec, ki ga izvajalec ni navedel v svoji ponudbi oziroma ni dogovorjen s to pogodbo oziroma izvajalec ni prijavil podizvajalca na način določen v tem poglavju, ima pravico odpovedati to pogodbo. Naročnik si pridržuje pravico, da lahko na kraju, kjer se dela izvajajo, kadarkoli preveri delavce kateregakoli od podizvajalcev, ki opravljajo dela. Vsi delavci so naročniku dolžni dati verodostojne podatke.

3. DOBAVA IN PREVZEM

7. člen

Rok za dobavo, namestitev in konfiguracijo ter primopredajo obeh požarnih pregrad (vključno s tehnično dokumentacijo) in izvedbo vseh storitev, ki so predmet te pogodbe, je **90 dni** od dneva podpisa pogodbe.

Pogodbeni rok iz prejšnjega odstavka velja pod pogojem, da je naročnik na dan začetka inštalacije opreme zagotovil električno, telekomunikacijsko in drugo infrastrukturo, ter da je izvajalcu omogočil pogoje za izvedbo del skladno z 18. členom te pogodbe.

Pogodbeni rok iz prvega odstavka tega člena se lahko izjemoma spremeni, če so nastopile posebne okoliščine, določene v 9. in 17. členu te pogodbe. Izvajalec mora spremembo roka dobave opreme predlagati naročniku najkasneje v treh delovnih dneh, ko izve za vzrok, zaradi katerega se lahko rok podaljša, sicer izgubi pravico do podaljšanja roka.

Izvajalec mora naročnika o nameravani dobavi pisno obvestiti vsaj 2 delovna dneva pred dobavo. V obvestilu mora navesti datum in uro možnega začetka dobave in način dobave.

Izvajalec mora hkrati z opremo naročniku izročiti še:
- pravilno izpolnjeno dobavnico;
- podpisane in potrjene garancijske liste;
- tehnično dokumentacijo in navodila za uporabo;
- licence, dokumentacijo in medije za programsko opremo, če je zahtevana;
- druge dokumente, če so zahtevani.

Prevzem opreme se izvede po uspešnem preizkusu opreme.

O prevzemu opreme se vodi prevzemni zapisnik, ki ga na podlagi pravilno izročene količinsko in kakovostno ustrezne opreme ter spremljajočih dodatkov in listin podpišeta pooblaščena predstavnika izvajalca in naročnika.

Ko je prevzemni podpisnik podpisan, pooblaščeni predstavnik naročnika podpiše dobavnico. Z dnem podpisa dobavnice je prevzem opravljen.

Oprema, za katero se bo ugotovilo, da odstopa od navedb v ponudbeni dokumentaciji, ali ni skladna z določili te pogodbe in specifikacijami, bo zavrnjena, zaradi česar bo izvajalec prešel v zamudo. Enako velja, če bo neskladnost ugotovljena za katerikoli dokument, ki bi moral biti opremi priložen. Zavrnitev bo označena na prevzemnem zapisniku.

4. ZAMUDA IN POGODBENA KAZEN

8. člen

Če prevzem opreme ne bo izveden v roku, določenem v prvem odstavku 7. člena te pogodbe, se šteje, da je izvajalec prišel v zamudo, razen če nastopijo okoliščine, določene v 9. in 17. členu te pogodbe.

Izvajalec je v primeru zamude pri dobavi, namestitvi in konfiguraciji opreme, ki ni posledica posebnih okoliščin iz 9. in 17. člena te pogodbe, dolžan plačati naročniku pogodbeno kazen v višini 0,5% od vrednosti nedobavljene opreme (vrednost z DDV) za vsak koledarski dan zamude.

V primeru zamude pri garancijskem vzdrževanju strojne opreme, ki nastane zaradi razlogov na strani izvajalca, je ta dolžan plačati pogodbeno kazen v višini 25,00 EUR za vsako uro zamude, če izvajalec ne odpravi napake v roku 6 ur po prejemu prijave napake, ali če v istem roku ne zagotovi funkcionalno enakovredne nadomestne opreme.

Če izvajalec zamuja z izvajanjem storitev vzdrževanja opreme toliko, da bi lahko naročniku nastala škoda ali da bi izvedba izgubila pomen, lahko naročnik nadomestno storitev naroči pri drugem izvajalcu na stroške zamudnika, lahko pa zahteva povrnitev dejanske škode ali unovči garancijo (menico) ali razdre pogodbo.

Ne glede na drugi in tretji odstavek tega člena se pogodbena kazen lahko obračuna največ do 10 % celotne pogodbene vrednosti z DDV.

Pogodbena kazen se plača oziroma izterja z unovčenjem finančnega zavarovanja za dobro izvedbo pogodbenih obveznosti in odpravo napak v garancijskem roku.

Če bi dejanska škoda presegla mejo, ki je v tej pogodbi določena kot največja vrednost pogodbene kazni, lahko naročnik zahteva povrnitev dejanske škode.

5. VIŠJA SILA

9. člen

Nobena od pogodbenih strank ni odgovorna za kršitev te pogodbe oziroma neizpolnitev katerekoli izmed svojih obveznosti iz razlogov, ki so nastali zaradi višje sile. Pod višjo silo se razumejo prekinitev delovanja telekomunikacijskih sredstev, napad na informacijske sisteme, naravne nesreče, požar, terorizem, vlom, oboroženi spopadi, ukrepi oblastnih organov in vsi drugi nepredvideni ter nepričakovani dogodki, na katere pogodbeni stranki ne moreta vplivati, ki nastopijo neodvisno od volje pogodbenih strank in ki jih pogodbeni stranki nista mogli predvideti ob sklepanju pogodbe ter kakorkoli vplivajo na izvedbo pogodbenih obveznosti.

Pogodbena stranka, ki je prizadeta zaradi kateregakoli dogodka iz prejšnjega odstavka, mora o tem takoj pisno obvestiti drugo pogodbeno stranko kakor tudi o ocenjenem obsegu in trajanju nezmožnosti za uresničevanje svojih obveznosti iz te pogodbe. Pogodbena stranka, ki je drugo pogodbeno stranko obvestila o nastopu višje sile, jo mora ob njenem prenehanju takoj pisno obvestiti. Pogodbena stranka, ki je prizadeta zaradi kateregakoli dogodka ali ukrepa iz tega člena, je še naprej odgovorna za izpolnjevanje vseh svojih obveznosti, ki jih tak dogodek ali ukrep ni prizadel.

6. GARANCIJA, VZDRŽEVANJE IN PODPORA

6.1. Garancijski pogoji

10. člen

Garancija za vso dobavljeno komunikacijsko strojno opremo je 36 mesecev in je všteta v ceno.

Za pripadajočo programsko opremo veljajo garancijski in licenčni pogoji, kot jih proizvajalec te opreme nudi za posamezne programske proizvode.

Garancijski rok začne teči od dneva podpisa dobavnice. Če je bila oprema v garancijskem roku zamenjana ali bistveno popravljena, začne garancijski rok znova in je dobavitelj / izvajalec dolžan izdati nov garancijski list.

Dobava in namestitev rezervnih delov ter vsi drugi stroški v zvezi s popravilom v času garancijskega roka bremenijo dobavitelja / izvajalca.

Dobavitelj / izvajalec ne jamči v naslednjih primerih:
- če naročnik z opremo ni ravnal po navodilih za uporabo, ki so priložena izdelkom,
- če je v izdelek posegla nepooblaščena oseba,
- če naročnik nestrokovno in malomarno ravna z izdelkom.

Garancija ne pokriva:
- okvar, povzročenih pri transportu po izročitvi blaga,
- mehanskih okvar, ki jih povzroči naročnik,
- okvar, povzročenih zaradi nihanja električne napetosti ali udara strele in prenapetostnega udara,
- okvar, povzročenih zaradi neustrezne temperature ali vlage,
- okvar, povzročenih zaradi višje sile.

6.2. Režim garancijskega vzdrževanja opreme

11. člen

Naročniku mora biti zagotovljena možnost, da lahko prijavi napako 24 ur in 7 dni v tednu.

V primeru nepravilnega delovanja programske opreme mora izvajalec naročniku nuditi tehnično pomoč in obvestiti proizvajalčev center za tehnično pomoč o zaznani napaki.

Ko proizvajalec dobavi novo različico programske opreme, mora izvajalec v dogovoru z naročnikom namestiti novo programsko opremo.

V primeru prijave okvare do 12. ure mora izvajalec okvaro na opremi odpraviti v istem delovnem dnevu, v primeru prijave okvare po 12. uri mora izvajalec okvaro na opremi odpraviti najpozneje naslednji delovni dan.

Vzdrževanje mora vključevati tudi:
1. vodenje vseh postopkov prijave, obravnave in odprave napak pri proizvajalcu,
2. neposreden (7x24x365) dostop do proizvajalčevega centra za tehnično pomoč,
3. dostop do novih verzij programske opreme,
4. pravico do vseh novih verzij programske opreme (v okviru funkcionalnosti), kot jih dobavlja proizvajalec opreme,
5. obveščanje naročnika o novih verzijah in spremembah v njih
6. vodenje dokumentacije vzdrževalnih posegov na opremi naročnika tako, da je naročniku zagotovljena možnost vpogleda v dokumentacijo preko interneta za čas trajanja pogodbe,
7. obveščanje naročnika o varnostnih problemih z obstoječimi verzijami programske opreme in takojšnja izvedba akcij v dogovoru z naročnikom, če obstaja varnostna ogroženost na opremi, ki jo ima naročnik;
8. dostop do tehnoloških informacij proizvajalca opreme v času trajanja te pogodbe.

Izvajalec mora ob sklenitvi pogodbe naročniku posredovati telefonsko število in elektronski naslov, na katerem je dosegljiv nadzornik sistema.

Komunikacija s klicnim centrom se mora izvajati v slovenskem jeziku; tehnično osebje, ki komunicira z naročnikom, mora tekoče govoriti slovensko.

Naročnik lahko kadarkoli med izvajanjem pogodbe preveri nivo zagotavljanja storitve.

12. člen

Odzivni čas na prijavo napake je čas, ki preteče od prejema naročnikove zahteve za pomoč oziroma od prejema prijave napake do trenutka, ko izvajalec začne z diagnosticiranjem in reševanjem/odpravljanjem napake.

Zaradi doslednega upoštevanja odzivnega časa in pravilnega izvajanja pogodbenih pravic in obveznosti pogodbeni stranki soglašata, da se šteje, da je izvajalec začel odpravljati napako v okviru odzivnega časa:

- v primeru manjše ali manj zahtevne okvare programske opreme, ko po telefonu pokliče prijavitelja napake in mu posreduje informacije o statusu reševanja prijavljene napake ali posreduje ustna navodila za odpravo napake;
- v primeru večje ali zahtevne okvare programske opreme, ko po telefonu pokliče prijavitelja napake in zahteva dodatne informacije, ki so potrebne za diagnosticiranje in odpravo napake, ter mu hkrati posreduje informacije o statusu reševanja prijavljene napake;
- v primeru okvare strojne opreme, ko vstopi v prostore na lokaciji naročnika in začne z diagnosticiranjem ter odpravljanjem okvare.

Izvajalec vodi evidenco opravljenih storitev na podlagi s strani naročnika podpisanih delovnih nalogov. Izvajalec dostavlja naročniku pisna poročila o vseh opravljenih storitvah na računalniški opremi.

V kolikor naročnik pisno ali v obliki elektronskega dokumenta ugotovi in obvesti izvajalca, da sta kakovost in obseg sporna, zadrži izplačilo zadnjega izdanega računa izvajalca in mora najkasneje v 8 dneh od datuma ugotovitve izvesti presojo, ki mora biti dokumentirana s poročilom v pisni ali elektronski obliki. Naročnik po potrebi lahko organizira komisijo za preverjanje kakovosti in obsega storitev v sestavi: naročnik, izvajalec, druge odgovorne osebe pri naročniku in zunanji svetovalec po potrebi, na način, da se opravi primerjava z vsebino pogodbe ter primerjava z dostavljenimi mesečnimi poročili. Rezultati teh preverjanj morajo biti dokumentirani in so tudi pogoj za realizacijo plačil.

Vsa strokovna dokumentacija, ki se nanaša na vzdrževanje in ki jo izvajalec na podlagi te pogodbe izroči naročniku, postane naročnikova last.

7. PRIJAVA NAPAKE

13. člen

Skrite napake na strojni opremi in skrite napake, povezane s storitvami namestitve in konfiguracije opreme se lahko prijavijo v enem (1) mesecu, ko je bila napaka odkrita, vendar najpozneje v roku enega (1) leta od primopredaje opreme.

Napake iz naslova garancije se lahko prijavijo kadar koli do izteka garancijskega roka.

Storitve iz naslova garancije, vzdrževanja in podpore se izvajajo na podlagi telefonske ali pisne zahteve naročnika. Prijave napak/okvar izvajalec sprejema po telefonu št. _____, ali prek e-naslova _____.

Izvajalec bo naročnika pisno obveščal o morebitnih spremembah telefonske številke in elektronskega naslova.

14. člen

Naročnik v skladu s svojim notranjim aktom določi javnega uslužbenca, ki bo pooblaščen za prijavo napake in komuniciranje z izvajalcem. Pooblaščeni javni uslužbenec mora:

- poznati telefonsko številko in naslov elektronske pošte izvajalca in dogovorjeni način komuniciranja z izvajalcem;
- poznati produkcijsko okolje naročnika;
- biti pooblaščen za odločanje v imenu naročnika glede storitev in za posredovanje informacij in podatkov, kot jih bo potreboval izvajalec pri reševanju zahtevkov,
- biti dosegljiv po telefonu ali e-pošti ali prisoten na lokaciji naročnika tudi po izteku rednega delovnega časa, če se popravilo izvaja neprekinjeno, vse dokler se napaka ne odpravi.

15. člen

V prijavi napake oziroma zahtevka za pomoč naročnik praviloma navede naslednje podatke:
- naziv in naslov naročnika, ime in priimek kontaktne osebe oziroma prijavitelja,
- datum in čas prijave,
- način obveščanja naročnika o statusu reševanja prijavljene napake,
- opis napake,
- vrsta napake (opis težave, opredelitev vprašanja, programska napaka, napaka v dokumentaciji, drugo),
- ponovljivost napake (opis zaporedja ukazov oziroma okoliščin, pri katerih pride do napake),
- obstoj pomožne rešitve in njen opis, v kolikor obstaja,
- druge podatke, ki jih sporazumno določita skrbnika pogodbe.

8. DRUGE PRAVICE IN OBVEZNOSTI POGODBENIH STRANK

16. člen

Izvajalec se zavezuje in naročniku jamči:
- da je vsa oprema tovarniško nova in zapakirana v originalni embalaži proizvajalca opreme;
- da oprema deluje brezhibno in nima stvarnih napak;
- da oprema nima pravnih napak;
- da oprema popolnoma ustreza vsem tehničnim opisom, karakteristikam in specifikacijam, ki so bila dana v okviru razpisne in ponudbene dokumentacije;
- da je oprema v skladu z zahtevano konfiguracijo ter da je namenjena slovenskemu trgu in opremljena z vsemi potrebnimi veljavnimi atesti in dovoljenji za uporabo v Republiki Sloveniji tako, da jo bo mogoče brez modifikacij uporabljati v Sloveniji ter jo v Sloveniji tudi vzdrževati;
- da doba zagotavljanja rezervnih delov za vso predmetno opremo (v zahtevani konfiguraciji) traja najmanj 5 let od dneva podpisa primopredajnega zapisnika;
- da bo naročnik po plačilu računa pridobil lastninsko pravico na opremi ter licenčne in druge pravice, skladno z licenčnimi pogoji proizvajalca opreme in zakonom, ki ureja avtorske pravice;
- da je oprema funkcionalno in tehnično združljiva z obstoječo opremo in informacijsko infrastrukturo naročnika, ter da njena implementacija naročniku ne bo povzročala dodatnih investicijskih stroškov oziroma nabav opreme ali stroškov izobraževanja zaposlenih;
- da bo svoje pogodbene obveznosti opravil strokovno, pravilno, vestno in kakovostno po pravilih stroke in v skladu s standardi proizvajalca opreme;
- da bo izpolnjeval vse pogodbene obveznosti v dogovorjenih rokih in na predviden način;
- da bo pisno opozoril naročnika na okoliščine, ki bi lahko otežile ali onemogočile kakovostno in pravilno izvedbo storitev;
- da bo izpolnil druge zahteve in obveznosti, določene v pogodbi in razpisni dokumentaciji.

17. člen

Izvajalec se obvezuje, da bo za opravljanje storitev zagotavljal ustrezne zmogljivosti v osebju, orodju, diagnostični opremi in rezervnih delih ter drugi opremi, potrebni za nemoteno izvajanje pogodbe, ter da bo napake odpravljal v pogodbenih rokih. Izvajalec ima pravico do podaljšanja pogodbenih rokov v primerih:

- dogodkov, ki so posledica višje sile;
- prekinitve izvajanja del na zahtevo naročnika;
- v primeru, da zamuda nastane kot posledica sprememb ali motenj v carinskem postopku, tako v Republiki Sloveniji kot v tujini (dogodki, na katere izvajalec ne more vplivati);
- če naročnik na svojih lokacijah ne zagotovi električne, telekomunikacijske in druge infrastrukture ter izvajalcu ne omogoči pogojev za izvedbo del skladno z 18. členom te pogodbe.

Izvajalec mora spremembo pogodbenega roka predlagati naročniku najkasneje v treh delovnih dneh, ko izve za vzrok, zaradi katerega se lahko rok podaljša, sicer izgubi pravico do podaljšanja roka.

Če naročnik ne izpolni svojih obveznosti, tako da izvajalec ne more opraviti dela na lokaciji naročnika, ali če izvajalec ugotovi, da je naročnik prijavil napako, ki ni predmet te pogodbe, je izvajalec dolžan pisno evidentirati situacijo in porabljeni čas, naročnik pa poravnati vse nastale stroške (porabljeni čas, potni stroški) po veljavnem ceniku izvajalca.

18. člen

Naročnik se obvezuje, da bo:

- zagotovil razpoložljivost potrebnih človeških in informacijskih virov;
- omogočil dostop izvajalcu do celotne dokumentacije in infrastrukture, če je to potrebno za izvedbo storitev, ki so predmet te pogodbe;
- zagotovil nemoten dostop do opreme, ki jo izvajalec potrebuje pri delu;
- priskrbel potrebne pravice za delo izvajalca na sistemu, uporabniška imena in gesla, če je to potrebno za izvedbo storitev;
- na zahtevo izvajalca v času posega v sistem zagotovil prisotnost administratorja sistema ali drugih (zunanjih) vzdrževalcev obstoječe opreme;
- izvajal preventivne in korektivne aktivnosti, ki jih bo priporočil izvajalec;
- redno plačeval finančne obveznosti, nastale po tej pogodbi.

Naročnik si bo prizadeval, da bo v skladu z možnostmi omogočil izvajalcu oddaljen dostop do programske opreme po elektronski poti oziroma prek spleta s ciljem učinkovitejšega izvajanja storitev.

19. člen

Naročnik ima status neposrednega uporabnika državnega poračuna, zato je to pogodbo sklenil v imenu in za račun Republike Slovenije. Pravico, ki jo pridobi na opremi ter z njo povezane pravice lahko naročnik neomejeno in brez kakršnekoli dolžnosti do izvajalca ali tretjega prenaša na druge organe v okviru državne uprave v skladu s predpisi, ki urejajo ravnanje s stvarnim premoženjem države. Naročnik s prevzemom in plačilom licenčne programske opreme pridobi pravico uporabe izdelka v skladu z licenčnimi pogoji, ki so del dokumentacije izdelka.

20. člen

Odstop oziroma prenos pogodbenih pravic in obveznosti na pravnega naslednika izvajalca ali tretjo osebo je možen samo s pisnim soglasjem naročnika in pod pogoji, določenimi v 4. točki prvega odstavka 95. člena ZJN-3.

9. PLAČILNI POGOJI

21. člen

Vse cene na enoto brez DDV, ki so navedene v ponudbi / predračunu, številka ____z dne_____, in v 2. členu te pogodbe, so fiksna ves čas trajanja te pogodbe.

Izvajalec bo naročniku izstavil račun za dobavljeno opremo in opravljene storitve namestitve in konfiguracije po uspešno opravljeni primopredaji opreme. Računu morata biti priložena zapisnik o prevzemu opreme in dobavnica, ki ju je ob izvajalčevi pravilni izpolnitvi pogodbenih obveznosti podpisal in žigosal pooblaščeni predstavnik naročnika.

Terminski načrt dobave opreme in faze izvedbe posameznih storitev sporazumno določita skrbnika, določena v prilogi __ te pogodbe.

Naročniku se račun pošilja na naslov: Uprava Republike Slovenije za javna plačila, Dunajska cesta 48, 1000 Ljubljana.

Račun se mora sklicevati na številko te pogodbe_____.

Račun mora biti izdan, poslan in vročen naročniku v elektronski obliki (v standardu e-SLOG), skladno z določbami Zakona o plačilnih in javnofinančnih storitvah (Uradni list RS, št. 85/25).

Naročnik prejeti račun po pregledu potrdi ali zavrne v roku 8 dni od prejema. Naročnik mora zavrnitev računa obrazložiti.

Rok plačila je največ 30 (trideset) dni. Plačilni rok začne teči naslednji dan po prejemu pravilno izstavljenega e-računa. Če zadnji dan roka sovpada z dnem, ki je po zakonu dela prost dan oziroma v plačilnem sistemu T2 ni opredeljen kot plačilni dan, se za zadnji dan roka šteje naslednji delavnik v Republiki Sloveniji oziroma naslednji plačilni dan v sistemu T2.

Vse dokler račun ni pravilno izstavljen v skladu z določbami te pogodbe, naročnik ni v zamudi. Izvajalec lahko v primeru zamude plačila zaračuna naročniku zakonite zamudne obresti v skladu z veljavnimi predpisi. Zamudne obresti zapadejo v plačilo 30 dni po prejemu obračuna obresti.

**Opomba naročnika: V primeru skupne ponudbe ali ponudbe s podizvajalci si naročnik pridržuje pravico, da ta člen dopolni ali doda nov člen, v katerem se podrobneje določijo pravice in obveznosti oziroma plačilni pogoji, vezani na sodelovanje drugih ponudnikov oziroma podizvajalcev ter neposredna plačila podizvajalcem, skladno z ZJN-3.*

10. FINANČNO ZAVAROVANJE

22. člen

Za finančno zavarovanje dobre izvedbe pogodbenih obveznosti in odprave napak v garancijskem roku mora izvajalec naročniku predložiti v osmih (8) dneh po podpisu te pogodbe tri (3) podpisane bianco menice in menično izjavo v višini 10 % skupne pogodbene vrednosti te pogodbe z DDV, veljavno od dneva izdaje in še 30 dni po prenehanju te pogodbe. Menična izjava mora biti izdana po vzorcu iz razpisne dokumentacije.

Finančno zavarovanje mora biti izdano po vzorcu iz razpisne dokumentacije.

Predložitev finančnega zavarovanja v skladu s prvim odstavkom tega člena je pogoj za veljavnost pogodbe in prevzem opreme.

Naročnik bo unovčil finančno zavarovanje:

- če izvajalec svojih obveznosti ne bo izpolnil v dogovorjenem obsegu, kvaliteti in rokih, opredeljenih v tej pogodbi,
- če izvajalec ne odpravi napak v garancijskem roku,
- če bo naročnik razdrl pogodbo zaradi kršitev na strani izvajalca,
- če bo naročnik razdrl pogodbo zaradi zamude, ki je nastala po izključni krivdi izvajalca, in ki je tudi po predhodnem pisnem opozorilu izvajalec ni odpravil oziroma predlagal za naročnika sprejemljiv alternativni plan,
- če bo izvajalec neutemeljeno zavrnil naročilo ali storitev ali če storitev odstopa od naročenega načina izvedbe,
- če bo naročnik prisiljen naročiti nadomestno storitev pri drugem gospodarskem subjektu na stroške izvajalca,
- če bo izvajalec neutemeljeno zavrnil plačilo pogodbene kazni za zamudo ali plačilo dejanske škode, ki je nastala naročniku,
- če bo izvajalec kršil zaupnost podatkov,
- ali v primeru druge kršitve pogodbene obveznosti, za katero je v tej pogodbi predvidena možnost unovčenja finančnega zavarovanja.

Naročnik lahko menico unovči, če je predhodno pisno (po pošti ali po elektronski pošti) obvestil izvajalca o kršitvi pogodbene obveznosti in zahteval izpolnitev v roku dveh (2) delovnih dni po prejemu obvestila, izvajalec pa ni ustrezno ukrepal. Če se kršitev pogodbene obveznosti ponovi, predhodno obvestilo ni več potrebno. Naročnik pa mora izvajalca o tem, da je unovčil menico, obvestiti po faksu, elektronski pošti ali pisno najkasneje 8 dni po dnevu, ko jo bila menica unovčena.

Naročnik, kot imetnik domicilirane menice, lahko odredi izvršitev plačilne transakcije na podlagi domicilirane menice v skladu z določbami 186. in 187. člena Zakona o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (Uradni list RS, št. 7/18, 9/18 – popr,. 102/20, 113/24 in 17/25 – ZPPDFT-2B). Menični znesek se nakaže na račun Republike Slovenije št. IBAN SI56 0110 0630 0109 972, s sklicem na številko, ki jo določi naročnik.

Naročnik se zavezuje, da skupna vrednost vseh unovčenih menic ne bo presegla 10 % celotne pogodbene vrednosti z DDV.

Izvajalec mora v primeru svojih statusnih sprememb oziroma prenosa izvajanja pogodbe na drug poslovni subjekt zagotoviti, da nov poslovni subjekt takoj predloži naročniku ustrezno finančno zavarovanje po tem členu pogodbe. V nasprotnem primeru lahko naročnik uveljavi izvajalčevo menično zavarovanje za dobro izvedbo pogodbenih obveznosti, s katerim razpolaga na podlagi te pogodbe.

Naročnik bo menice, če jih ne bo uporabil, vrnil izvajalcu v 60 dneh po prenehanju veljavnosti te pogodbe.

11. INFORMACIJSKA VARNOST

23. člen

(1) Pogodbeni stranki se obvezujeta, da bosta varovali podatke o izvorni in strojni kodi računalniških programov in zaupne podatke tehničnega in poslovnega značaja, do katerih imata dostop pri izvajanju te pogodbe (npr. rezultati varnostnih testov, poročila varnostnega pregleda, poročila o varnostnih incidentih ipd.), ter podatke, za katere je očitno, da bi nastala občutna škoda, če bi zanje izvedela nepooblaščena oseba, in sicer kot poslovno skrivnost izvajalca oziroma uradno skrivnost naročnika skozi ves pogodbeni rok ter še najmanj deset (10) let po preteku le-tega.

(2) Naročnik kot upravljavec zbirke osebnih podatkov vodi, vzdržuje in nadzoruje zbirke osebnih podatkov in evidenco obdelav osebnih podatkov na način in pod pogoji, določenimi v Uredbi (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L št. 119 z dne 4. 5. 2016; v nadaljnjem besedilu: GDPR) in v Zakonu o varstvu osebnih podatkov (Uradni list RS, št. 163/22, 40/25 – ZInfV-1 in 10/26 – ZP-1L; v nadaljnjem besedilu: ZVOP-2).

(3) Osebni podatki zaposlenih, navedenih v tej pogodbi ali njenih prilogah, se obdelujejo za potrebe izvajanja te pogodbe v skladu z 48. členom Zakona o delovnih razmerjih (Uradni list RS, št. 21/13, s spremembami in dopolnitvami) in 92. členom ZVOP-2.

(4) Pogodbeni stranki sporazumno ugotavljata, da aktivnosti izvajalca pri vzdrževanju opreme ne predstavljajo pogodbene obdelave osebnih podatkov in da izvajalec ne nastopa v vlogi obdelovalca po 28. členu GDPR.

(5) Pogodbeni stranki se obvezujeta, da bosta zagotovili tehnične, organizacijske, fizične in kadrovske pogoje za varno obravnavanje osebnih podatkov, davčne tajnosti in poslovne skrivnosti, uradne skrivnosti in tajnih podatkov (v nadaljevanju: varovani podatki), skladno z zahtevami in standardi področnih predpisov, ki urejajo varovanje podatkov in informacijsko varnost.

(6) Za označevanje podatkov oziroma dokumentov, medijev ali nosilcev podatkov, se uporabljajo posebne varnostne oznake, določene z zakonom ali podzakonskim aktom ali notranjim aktom pogodbene stranke, če so izpolnjeni predpisani pogoji za določitev statusa varovanega podatka.

(7) Če pri izvajanju te pogodbe nastane potreba po dostopu do dokumentov in tajnih podatkov stopnje »INTERNO«, mora izvajalec predhodno (najpozneje pred dostopom do podatkov) opraviti varnostno preverjanje in pridobiti varnostno dovoljenje v skladu z določbami Zakona o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11, 8/20 in 18/23 – ZDU-1O).

(8) Izvajalec mora označiti svoje podatke, dokumente ali dele dokumentov, ki so zaupni in ki izpolnjujejo pogoje in zahteve za poslovno skrivnost v skladu z 2. členom Zakona o poslovni skrivnosti (Uradni list RS, št. 22/19; v nadaljnjem besedilu: ZPosS), ali naročniku predložiti pisni sklep ali drug akt o določitvi poslovne skrivnosti. Pri tem ni dovoljeno neopravičeno ali pavšalno označevati zaupnosti tistih dokumentov, ki so javnega značaja, skladno s 35. členom ZJN-3 in tretjim odstavkom 2. člena ZPosS ter zakonom, ki ureja dostop do informacij javnega značaja.

(9) Dostop do varovanih podatkov imajo samo tiste osebe, ki morajo imeti vpogled v te podatke po svoji službeni dolžnosti zaradi uresničevanja javnega naročila, ki je predmet te pogodbe. Seznam teh delavcev je priloga 2 te pogodbe. Izjavo o varovanju podatkov, ki je priloga 3 te pogodbe, morajo podpisati delavci izvajalca, ki sodelujejo pri izvajanju naslednjih pogodbenih del:
- konfiguriranje, implementacija, tehnična podpora in nadgradnja programske opreme,
- dela, ki se opravljajo v prostorih naročnika,
- dela, kjer se prihaja v stik s kakršnimikoli podatki naročnika ali drugih državnih organov in uporabnikov naročnikovih storitev.

(10) Izvajalec zagotavlja, da so bili vsi njegovi delavci, navedeni v prilogi 2 te pogodbe, vključeni v programe ozaveščanja in usposabljanja s področja informacijske varnosti, ter da so seznanjeni:
- s svojimi vlogami in odgovornostmi na področju informacijske varnosti,
- z varnostnimi zahtevami, določenimi v veljavnih predpisih Republike Slovenije, notranjih aktih izvajalca in v tej pogodbi,
- z načinom izvajanja svojih varnostnih nalog po tej pogodbi,

- s pravnimi posledicami v primeru kršitev dolžnosti varovanja podatkov (delovno-pravne sankcije, materialna in odškodninska odgovornost, prekrškovna odgovornost, odgovornost za kazniva dejanja)

(11) Izvajalec mora seznam in izjave vseh delavcev iz 9. odstavka tega člena izročiti naročniku hkrati s podpisanim izvodom te pogodbe. Izvajalec ob vsakokratni kadrovski spremembi pripravi novo verzijo seznama delavcev in jo posreduje v seznanitev naročniku skupaj z izjavo o varstvu podatkov, podpisano s strani nadomestnega delavca.

(12) Izvajalec mora naročnika takoj obvestiti o vsakem disciplinskem ali drugem postopku, zaradi kršitev delovnih obveznosti, ki ga je zoper delavce sprožil v zvezi z izvajanjem pogodbenih del.

(13) Izvajalec se zavezuje, da bo vse naročnikove dokumente, medije in druge nosilce varovanih podatkov (vključno s tistimi, ki nimajo posebne varnostne oznake), do katerih ima dostop pri izvajanju te pogodbe, varoval z enakimi varnostnimi ukrepi, kot veljajo za varstvo poslovne skrivnosti, razen če ta pogodba za posamezne varovane podatke določa strožje pogoje in varnostne zahteve.

(14) Izvajalec mora tehnično in drugo zaupno dokumentacijo v fizični obliki, ki jo prejme od naročnika, hraniti v protivlomnem in ognjevarnem sefu/trezorju.

(15) Izvajalec mora prostore, kjer se izvajajo pogodbena dela in v katerih so nameščene za delovanje izvajalca ključne informacijske naprave (strežniki, pomnilniške naprave, telefonske centrale, omrežna vozlišča in drugo), ustrezno zaščititi pred vlomom oziroma nepooblaščenim dostopom in vplivi okolja, kot so požar, vdor vode, izpad električnega omrežja, onesnaženje, temperaturna nihanja, elektromagnetne motnje in drugo ter urediti in zagotoviti ustrezno varnostno opremo in opremo pristopne kontrole v skladu z veljavnimi predpisi, standardi, navodili proizvajalcev informacijske opreme in lastno oceno tveganja ter zahtevami naročnika skladnimi s to pogodbo in določenimi na podlagi ugotovitev ogleda teh prostorov.

(16) Varovani podatki naročnika, ki so pri izvajanju te pogodbe izvirno nastali v digitalni obliki ali bili pretvorjeni v digitalno obliko, se obdelujejo in hranijo izključno v okviru informacijskega sistema naročnika (z zagotovljenim oddaljenim dostopom), skladno z naslednjimi zahtevami:
- vstopne točke v naročnikovo komunikacijsko omrežje so pod nadzorom skrbnika komunikacijskega omrežja oziroma informacijskega sistema;
- naročnik s politiko upravljanja omrežja določa načine povezav, protokole, storitve, mehanizme varovanja in nadzora nad omrežjem ter dovoljeno uporabo;
- overjanje uporabnikov za dostop do naročnikovega informacijskega sistema in dostop sta izvedena z avtentikacijskim sredstvom, ki ga določi skrbnik sistema;
- dostop v bazo podatkov, vodeno v informacijskem sistemu naročnika, je avtoriziran z gesli;
- do naročnikovega komunikacijskega omrežja oziroma do strojne in programske opreme, ki je predmet vzdrževanja in nadgradnje, imajo dostop javni uslužbenci naročnika in pogodbeni izvajalci, ki so pridobili soglasje skrbnika informacijskega sistema, do katerega potrebujejo dostop;
- uporabnik prejme avtentikacijsko sredstvo in namensko programsko opremo po tem, ko skrbnik naročnikovega komunikacijskega omrežja odobri dostop;
- prepovedan je izvoz varovanih podatkov oziroma njihov prenos v digitalni obliki iz informacijskega sistema naročnika v informacijski sistem izvajalca ali njegovih podizvajalcev ali v »računalniški oblak« ter nadaljnja obdelava izven informacijskega sistema naročnika. Ta prepoved velja tudi v primeru, ko izvajalec odpravlja napako na podlagi prijave naročnika.

(17) Izvajalec v izdelke, ki so predmet dobave in vzdrževanja, ne sme vgraditi nobenega mehanizma oziroma zlonamernega programa, ki bi mu omogočal v informacijskem sistemu naročnika

kakršenkoli iznos ali nedovoljeno hranjenje podatkov, spreminjanje podatkov ali programske opreme, dostop do kateregakoli dela računalniškega sistema brez vednosti ali nadzora naročnika.

(18) Izvajalec zagotavlja, da ima vzpostavljen sistem nadzorstva, ki preprečuje dostop nepooblaščenih oseb do njegovih varovanih prostorov in informacijskega sistema, ki ga uporablja za izvajanje storitev po tej pogodbi, skladno z naslednjim zahtevami:

- v prostore, kjer se izvajajo pogodbena dela ali hrani zaupna dokumentacija, ali se z njo prihaja v stik, lahko vstopajo le pooblaščeni delavci izvajalca. Druge osebe lahko vstopijo v te prostore le na podlagi dovoljenja izvajalca ali v spremstvu pooblaščene osebe in so evidentirane na posebni listi (dnevnik vstopov), na kateri je naveden ime in priimek, datum, čas prihoda in odhoda, namen vstopa in organizacija, ki ji pripada. Dnevniki vstopov in morebitni videoposnetki se lahko razkrijejo naročniku v minimalnem obsegu, ki je potreben za nadzor nad izvajanjem te pogodbe, ter hranijo največ eno leto po poteku leta v katerem so nastali, nato se zbrišejo, razen če področni zakon določa drugačen rok hrambe;
- vsak posameznik, ki prejme sredstva za dostop do varovanih območij in prostorov (npr. ID kartica, ključ ipd.), ta sredstva varno in skrbno hrani, skladno z navodili, ki jih izda izvajalec. Sredstva za dostop niso prenosljiva na tretjo osebo in se vrnejo, ko prenehajo razlogi, zaradi katerih so bila dodeljena;
- kraja, izguba, zloraba ali sum zlorabe sredstva za dostop se obravnava kot incident informacijske varnosti, ki se zabeleži in o njem poroča osebi, ki je pri izvajalcu odgovorna za informacijsko varnost;
- dostop do informacij, storitev in upravljanja informacijskih sistemov je mogoč na podlagi dostopnih pravic. Te dodeljuje, spreminja in ukinja skrbnik informacijskega sistema ali upravljavec informacijskega sistema na podlagi pisne zahteve skrbnika informacijskega sistema;
- dostopne pravice se dodelijo tako, da omogočajo uporabniku dostop do najmanjšega možnega nabora storitev, funkcij in informacij, ki so potrebne za opravljanje njegovih nalog.
- ločijo se uporabniške in upravljavske dostopne pravice;
- pravice do dostopa do informacijskega sistema, informacij in storitev se redno preverja in posodablja. Dostopne pravice se nemudoma spremeni ali ukine, če uporabnik zamenja delovno mesto, prekine delovno ali pogodbeno razmerje ali če se spremeni ali preneha potreba po dostopu;
- dostopne pravice uporabnikov se dokumentira. Razvidi vsebujejo informacije o identiteti uporabnika, o ravni oziroma vrsti dostopnih pravic in o tem, kdaj je bil dostop odobren, kdaj so bile dostopne pravice spremenjene in kdaj so bile dostopne pravice odvzete;
- informacijski sistem uporablja najmanj enega od naslednjih postopkov avtentikacije uporabnikov:
    - avtentikacijo, temelječo na geslu, pri kateri informacijski sistem zagotavlja uporabo močnih / varnih gesel,
    - avtentikacijo, temelječo na infrastrukturi javnih ključev, pri kateri informacijski sistem preveri veljavnost certifikata s preverjanjem certifikacijske poti in informacije o statusu certifikata, zagotovi pooblaščen dostop do odgovarjajočega zasebnega ključa in poveže avtenticirano identiteto z imetnikom računa,
    - osebno registracijo ali registracijo prek zaupanja vredne tretje stranke, pri kateri se zahteva, da poteka registracijski postopek za prejem avtentikacije osebno ali prek zaupanja vredne tretje stranke pred registracijskim organom s pooblastilom pristojne osebe izvajalca,
    - avtentikacijo, temelječo na varnostnem žetonu.
- za oddaljeni dostop informacijski sistem uporabljajo večfaktorsko avtentikacijo tako, da je eden od faktorjev zagotovljen z napravo, ki je ločena od sistema, do katerega se dostopa;
- za zagotavljanje varnosti gesel se izvajajo naslednji ukrepi:
    - uporabniki so seznanjeni z zahtevami, vezanimi na dolžino, oblikovanje in strukturo gesel;

- uporabniki ne smejo uporabljati istih gesel za službeno in zasebno uporabo;
- gesla, ki so bila ali se zanje sumi, da so bila razkrita ali ukradena, se nemudoma spremenijo;
- vsa gesla uporabniških računov so osebna in se ne smejo deliti z drugimi osebami;
- vsa gesla se obravnavajo kot zaupni podatki. Nešifrirana gesla razen začasnih se ne smejo vključiti v sporočilo e-pošte ali sporočila drugih sporočilnih sistemov. Gesla razen začasnih se ne smejo razkriti po telefonu. Gesla se ne smejo zapisovati in hraniti na prosto dostopnih mestih v pisarni. Gesla se ne smejo hraniti v datoteki na računalniškem sistemu ali prenosni napravi v nešifrirani obliki. Začasna gesla, ki se dodelijo uporabniku, mora uporabnik spremeniti v najkrajšem možnem času.
- aplikacije morajo zagotoviti avtentikacijo vsakega posameznega uporabnika in ne skupin. Aplikacije ne smejo hraniti gesel v nešifrirani obliki ali obliki, ki bi bila preprosto povračljiva. Aplikacije ne smejo pošiljati gesel prek omrežja v nešifrirani obliki.

(19) Izvajalec zagotavlja, da ima vzpostavljen sistem nadzora namestitve in uporabe informacijskih naprav v svojem informacijskem sistemu, ki ga uporablja za izvajanje storitev po tej pogodbi, skladno z naslednjimi zahtevami:

- vse informacijske naprave se namestijo in zaščitijo tako, da je tveganje zaradi okoljskih nevarnosti in nepooblaščenega dostopa kar najmanjše;
- informacijske naprave nameščajo le za to usposobljene in pooblaščene osebe v skladu z veljavnimi predpisi, standardi in pogodbenimi določili;
- prosti priključki komunikacijske opreme v prostorih ne smejo omogočati nepooblaščenega dostopa do omrežja;
- informacijske naprave izvajalca so namenjene za službeno uporabo. Delavci lahko informacijske naprave izjemoma uporabljajo za zasebne namene, vendar taka uporaba ne sme ogrožati informacijske varnosti in mora biti v skladu z omejitvami, ki jih določi zakoniti zastopnik ali pooblaščena oseba izvajalca;
- delavci svojih zasebnih informacijskih naprav ne smejo povezovati v informacijski sistem izvajalca ali informacijski sistem naročnika. Z njimi ni dovoljeno prenašati podatkov izvajalca in naročnika ali jih hraniti na njih;
- ne glede na določbo prejšnje alineje se zasebne informacijske naprave, ki ustrezajo tehnološkim standardom in zmogljivostim informacijskih sistemov izvajalca in naročnika, lahko izjemoma uporabljajo tudi za službene namene, če so upoštevane operativne zahteve za zagotavljanje informacijske varnosti in uporaba take informacijske naprave ne povečuje tveganja informacijske varnosti;
- povezovanje in uporabo zasebnih informacijskih naprav zagotovi upravljavec informacijskega sistema, s katerim se zasebne naprave povezujejo, na podlagi pisne odobritve skrbnika tega informacijskega sistema;
- če se v omrežju zazna nedovoljena naprava, se naprava odstrani ali onemogoči, zadeva pa se obravnava kot varnostni incident v skladu z določbami notranjega akta izvajalca;
- prenos podatkov in dokumentov v drug informacijski sistem ali napravo je dovoljen le ob pisnem soglasju skrbnika izvornega informacijskega sistema in pod pogojem, da je v sprejemnem informacijskem sistemu ali napravi zagotovljena najmanj enaka raven varovanja zaupnosti in celovitosti teh podatkov oziroma dokumentov kot v izvornem informacijskem sistemu. Raven varovanja zaupnosti in celovitosti prenesenih podatkov in dokumentov v sprejemnem informacijskem sistemu in morebitno uvedbo dodatnih varnostnih ukrepov določi skrbnik izvornega informacijskega sistema, skrbnik sprejemnega informacijskega sistema pa mora tako raven varovanja zagotoviti.

(20) Izvajalec zagotavlja, da njegovi notranji akti zavezujejo delavce k izvajanju naslednjih varnostnih ukrepov:

- delavci ne smejo puščati nosilcev varovanih podatkov na odprtih površinah pisarniške opreme ali drugih mestih, kjer so dostopni nepooblaščenim osebam;
- izven delovnega časa izvajalca in kadar delavci niso fizično prisotni v prostoru, se vsa pisarniška oprema, kjer se hranijo varovani podatki, zaklene ali drugače zavaruje, informacijske naprave pa fizično ali programsko zaklenejo oziroma zavarujejo;
- v času, ko delavec ni prisoten, mora biti zaslon informacijske naprave, ki se nahaja v pisarniškem okolju, zaklenjen ali naprava odjavljena;
- delavci uporabljajo sistem elektronske pošte in internet v skladu z nameni, pogoji in omejitvami ter varnostnimi zahtevami, določenimi v notranjem aktu izvajalca.

(21) Izvajalec zagotavlja, da je njegov informacijski sistem, ki ga uporablja za izvajanje storitev po tej pogodbi, zaščiten pred škodljivo programsko opremo in prenosno kodo, ter da izvaja naslednje varnostne ukrepe:

- prenos, nameščanje in uporaba neodobrene programske opreme niso dovoljeni in je delavcem / uporabnikom onemogočeno nameščanje programske opreme na delovne postaje;
- na strežnikih, delovnih postajah in prenosnih informacijskih napravah je nameščena in se redno posodablja programska oprema za zaznavo in odpravo škodljive programske opreme, ki je namenjena za pregledovanje informacijskih naprav in podatkovnih medijev in zagotavlja:
    - preverjanje datotek na magnetnih ali optičnih medijih in datotek, prejetih prek omrežij, preden se uporabijo, glede okuženosti s škodljivo programsko opremo,
    - preverjanje priponk elektronske pošte in snetih datotek, preden se uporabijo, na poštnih strežnikih, namiznih računalnikih, ob vstopu v omrežja,
    - preverjanje spletnih strani glede vsebovanja škodljive programske opreme;

- v primeru okužbe ali suma okužbe s škodljivo programsko opremo delavec / uporabnik takoj preneha uporabljati prizadete informacijske naprave in poroča o dogodku osebi, ki je pri izvajalcu odgovorna za informacijsko varnost;
- škodljivo programsko opremo odstrani za to usposobljeni upravljavec informacijskega sistema;
- upravljavec informacijskega sistema se na dogajanja v informacijskem sistemu dosledno odziva s ciljem zagotavljanja učinkovitega in varnega delovanja informacijskega sistema;
- zapisi o uporabi in delovanju informacijskega sistema se sprotno beležijo v dnevnike dogodkov;
- dnevniki dogodkov omogočajo prepoznavo procesov in oseb, ki so uporabljale informacijski sistem, pregledovale podatke, jih spreminjale ali brisale;
- dnevniki dogodkov se uporabljajo za ugotavljanje ranljivosti, napak in ustreznosti nadzorstev ter za reševanje incidentov in ugotavljanje zlorab;
- če dnevnik dogodkov vsebuje informacije, ki so uporabne za preiskavo varnostnega incidenta ali za preverjanje uporabe in delovanja informacijskega sistema, ali informacije, ki bi jih bilo mogoče uporabiti kot dokaz v disciplinskih ali kazenskih postopkih, se ta dnevnik ohrani za obdobje, določeno v veljavnih predpisih in notranjih aktih izvajalca.

(22) Izvajalec se zavezuje, da bodo njegovi delavci pri delu in gibanju v prostorih naročnika (npr. če se namestitev in konfiguracija opreme ali odprava napake ali druga storitev izvaja na lokaciji naročnika), upoštevali pravila in predpise oziroma notranje akte naročnika, ki urejajo informacijsko varnost, pod pogojem, da bodo s temi akti predhodno seznanjeni.

(23) Izvajalec se zavezuje, da bodo njegovi delavci, ki opravljajo delo na lokaciji izvajalca ali delo na daljavo, upoštevali veljavne predpise, standarde, certifikate ter notranje akte izvajalca, ki urejajo varovanje podatkov, prostorov, strojne in programske ter komunikacijske opreme in infrastrukture.

(24) Izvajalec zagotavlja, da je vzpostavil postopke za zaznavo dogodkov in incidentov informacijske varnosti v svojem informacijskem sistemu in delovnem okolju ter postopke obvladovanja incidentov informacijske varnosti, ki vključujejo:

- spremljanje, zaznavanje, analiziranje in poročanje o dogodkih in incidentih informacijske varnosti,
- beleženje aktivnosti obvladovanja incidentov in
- odziv na incidente, vključno s postopki za stopnjevanje ukrepov informacijske varnosti, postopki za nadzorovano obnovo po incidentu in komunikacijo z notranjimi ali zunanjimi osebami ali organizacijami.

(25) Izvajalec mora naročnika oziroma osebo, odgovorno za informacijsko varnost, takoj obvestiti o vsakem varnostnem incidentu ali dogodku (npr. sprožitev protivlomnega ali protipožarnega alarma, vdor v informacijski sistem, zaznane motnje ali napake pri delovanju sistema, dogodki ob izvedbi servisnih oziroma vzdrževalnih posegov na informacijski in komunikacijski infrastrukturi, nepooblaščen dostop do podatkov in informacijskih sredstev, škodljivo programje, človeška napaka, kršitev varnostnih pravil, naravna ali druga nesreča, javni nemiri, vlom, fizična poškodba ipd.) pod pogojem, da varnostni incident ali dogodek lahko ogrozi nemoteno delovanje opreme, ki je predmet te pogodbe, ali informacijsko varnost naročnika v zvezi s predmetom te pogodbe ali opravljanje plačilnih in drugih storitev naročnika ali nemoteno opravljanje izvajalčevih pogodbenih obveznosti. V obvestilu o varnostnem incidentu ali dogodku morajo biti podani:

- opis dogodka informacijske varnosti,
- datum in čas zaznave dogodka,
- kdo je dogodek zaznal,
- taksonomija-klasifikacija incidenta (prva ocena),
- ocena stopnje nevarnosti,
- ocena možnega vpliva,
- ocena stopnje incidenta,
- ocena možne izgube podatkov, če je znana,
- druge podatke, pomembne za identifikacijo in odpravo posledic dogodka informacijske varnosti.

(26) Izvajalec se zavezuje, da bo naročniku razkril vse morebitne nove ali spremenjene okoliščine in dejstva, ki bi lahko vplivale na njegovo sposobnost za zakonito, uspešno in pravočasno izvedbo naročila oziroma te pogodbe. To vključuje predvsem, ne pa izključno, obveščanje naročnika o naslednjih dogodkih in dejstvih:

- zaznanih pomembnih (operativnih) tveganjih v zvezi z izvajanjem te pogodbe;
- vsakršnih aktivnostih oziroma nameri izvajalca, da se statusno ali lastniško prestrukturira;
- finančni nestabilnost izvajalca in uvedbi postopkov zaradi insolventnosti oziroma postopka likvidacije;
- nezmožnosti zagotavljanja storitev v dogovorjeni kakovosti in dogovorjenem času ali nedoseganja drugih dogovorjenih pogodbenih obveznosti;
- prenehanju ali spremembi statusa pri proizvajalcu ali principalu opreme (npr. prenehanje statusa pooblaščenega partnerja oziroma serviserja, prenehanje veljavnosti certifikatov ipd.), ki vplivajo za sposobnost zagotavljanja storitev, ki so predmet te pogodbe;
- ravnanjih, ki so neskladna s standardi, predpisi in zakoni, ki se uporabljajo pri izvajanju storitev po tej pogodbi;
- tehnološki zastarelosti;
- odhodu ključnih kadrov, ki sodelujejo pri izvedbi predmetnih storitev;
- vsakršnih sodnih, upravnih ali drugih uradnih postopkih ter kakršnih koli civilnih tožbah, ugotovitvah revizorjev, odločitvah nadzornih organov in podobno, ki se posredno ali neposredno nanašajo na predmet te pogodbe in/ali bi lahko materialno vplivali na sposobnost, da izpolni svoje obveznosti iz te pogodbe.

(27) V primeru nastopa spremenjenih okoliščin, navedenih v prejšnjem odstavku, lahko izvajalec v roku, ki ga bo določil naročnik, predloži dokaze, da je sprejel zadostne ukrepe, s katerimi lahko dokaže svojo zanesljivost kljub obstoju spremenjenih okoliščin. Če izvajalec ne bo predložil dokazov ali če jih bo, pa bo naročnik ocenil, da ti ukrepi ne zadoščajo, lahko naročnik odpove to pogodbo in začne nov postopek javnega naročanja ter sklene pogodbo z drugim izvajalcem. V tem primeru mora izvajalec v prehodnem obdobju (do izteka odpovednega roka in še najmanj 3 mesece po prenehanju veljavnosti pogodbe) sodelovati z naročnikom pri izvedbi vseh aktivnosti, ki so potrebne za prenos vzdrževalnih storitev na novega izvajalca, ter zagotoviti ustrezna uporabniška navodila in tehnično dokumentacijo, če je to potrebno za nemoteno vzdrževanje opreme, ki je predmet te pogodbe. Storitve iz predhodnega stavka štejejo za dodatne storitve, ki jih izvede izvajalec, ker so potrebne, čeprav niso bile vključene v prvotno javno naročilo, in zamenjava izvajalca ni mogoča iz tehničnih razlogov ter bi naročniku povzročila velike nevšečnosti in znatno podvajanje stroškov.

(28) Izvajalec se zavezuje, da bo zagotavljal revizijsko sled dostopov do varovanih podatkov, ki omogoča naknadno ugotavljanje uporabnika, časa in vrste izvedene aktivnosti. Revizijske sledi se hranijo v času izvajanja pogodbe in še najmanj 10 let po njenem prenehanju oziroma skladno z veljavno zakonodajo. Po prenehanju pogodbe izvajalec vse varovane podatke na zahtevo naročnika vrne ali trajno izbriše oziroma uniči ter naročniku posreduje pisno potrdilo ali drug ustrezen dokaz o opravljenem uničenju.

(29) Upravljanje izmenljivih nosilcev podatkov (USB ključ, polprevodniški disk, CD, DVD, trdi disk, magnetni trak ipd.) se izvaja v skladu z naslednjimi zahtevami in varnostnimi ukrepi:

- nosilci podatkov neznanega ali sumljivega izvora se ne smejo uporabljati in se predajo vodji informacijske varnosti, ki zagotovi preveritev izvora in morebitne okuženosti z zlonamerno programsko kodo;
- izguba ali kraja izmenljivih nosilcev podatkov se obravnava kot varnostni incident in se takoj prijavi osebi, odgovorni za informacijsko varnost;
- če izmenljivi nosilec podatkov vsebuje tehnično dokumentacijo in druge zaupne podatke oziroma dokumente, se uporabijo primerni postopki za šifriranje (kriptografski algoritmi, programska in strojna kriptografska oprema ter sistemi za upravljanje ključev), ki ustrezajo varnostnim zahtevam, temelječim na oceni tveganja;
- naročnik lahko zahteva, da se posamezni izmenljivi nosilci podatkov hranijo v protivlomnem in ognjevarnem sefu/trezorju;
- okvarjene nosilce podatkov mora izvajalec pod nadzorom naročnika uničiti ali trajno izbrisati, tako da pod nobenim pogojem ni možno obnoviti podatke, ki jih je nosilec vseboval;
- če vzdrževalnih del ni mogoče opraviti na lokaciji naročnika, se mora nosilce podatkov iz računalniške opreme odstraniti in jih varno shraniti. V primeru, da to ni mogoče, mora biti postopek vzdrževanja s strani naročnika nadzorovan. Če je v okvari nosilec podatkov, se le tega iz opreme odstrani. Pod nadzorom odgovorne osebe s strani naročnika se izvede poskus restavriranja podatkov na drug medij. V primeru, da je nosilec okvarjen do te mere, da podatkov oziroma dela podatkov ni mogoče restavrirati, se o tem napiše zapisnik.

(30) Izvajalec ima zagotovljeno varnost prenosnih informacijskih naprav (računalnik, dlančnik, osebni organizator, pametni telefon ali podobna prenosna elektronska naprava, ki lahko hrani, obdeluje, prikazuje ali elektronsko prenaša podatke; v nadaljnjem besedilu: prenosne informacijske naprave) in varnost dela na terenu v skladu z naslednjimi zahtevami:

- uporabniki prenosnih informacijskih naprav so seznanjeni z dodatnimi tveganji, ki so jim izpostavljene prenosne informacijske naprave, kadar jih odnesejo iz varovanega pisarniškega okolja;
- uporabniki so odgovorni za redno zaščitno kopiranje podatkov, ki so shranjeni na prenosnih informacijskih napravah;
- v primeru izgube, poškodbe, okvare ali kraje prenosne informacijske naprave uporabnik o tem nemudoma obvesti osebo, odgovorno za informacijsko varnost;

- hrambo zaupnih podatkov na prenosnih informacijskih napravah pisno odobri skrbnik informacijskega sistema, v katerem se ti podatki izvorno obravnavajo. Te podatke se ustrezno zavaruje s šifriranjem;
- oddaljen dostop do izvajalčevega ali naročnikovega komunikacijskega omrežja uporabnikom prenosnih informacijskih naprav je na voljo pod pogojem, da za to obstaja poslovna potreba. Uporabnik sme uporabljati le varni odobreni način povezave v komunikacijsko omrežje iz nevarovanih omrežij, temelječ na mehanizmih navideznega zasebnega omrežja, ki vključuje zanesljive postopke identifikacije in avtentikacije;
- prenosne informacijske naprave, ki se nahajajo zunaj pisarniških prostorov, morajo biti ves čas osebno nadzorovane ali varno shranjene;
- uporabniki prenosnih informacijskih naprav na sredstvih javnega prevoza, v čakalnicah, javnih lokalih in na drugih javnih mestih ne smejo izmenjevati varovanih podatkov ali dostopati do njih, če ne morejo preprečiti prisluhov in vpogledov na zaslon. Na prenosnih informacijskih napravah, ki omogočajo govorno komunikacijo, se ne opravlja zaupnih razgovorov, če se uporabljajo periferne enote z neustrezno zaščiteno ali nezaščiteno brezžično povezavo;
- povezave prek javnih brezžičnih (Wi-Fi) dostopnih točk so omejene na aktivnosti, ki ne vključujejo obravnave varovanih podatkov;
- na prenosnih informacijskih napravah, ki imajo vgrajena nezaščitena ali neustrezno zaščitena komunikacijska vrata in hranijo varovane podatke, morajo biti ta vrata onemogočena.

(31) Vsaka pogodbena stranka določi osebo, odgovorno za informacijsko varnost. Podatki o osebah, odgovornih za informacijsko varnost, so priloga 4 te pogodbe. Osebi, odgovorni za informacijsko varnost, sta zadolženi za:
- obravnavo dogodkov in incidentov informacijske varnosti, ki nastanejo v zvezi z izvajanjem te pogodbe,
- preverjanje skladnosti delovanja izvajalca z varnostnimi zahtevami, določenimi v tej pogodbi,
- sodelovanje pri usklajevanju varnostnih ciljev in ukrepov izvajalca in naročnika,
- izvedbo ocenitve tveganj informacijske varnosti in upravljanje teh tveganj ter
- pripravo poročil, operativnih navodil, smernic in varnostnih priporočil v zvezi z izvajanjem te pogodbe.

(32) Za elektronsko podpisovanje te pogodbe in drugih digitalnih dokumentov, vezanih na izvajanje te pogodbe, se uporablja kvalificirano potrdilo za elektronski podpis, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L, št. 257 z dne 28. 8. 2014, str. 73) in Zakona o elektronski identifikaciji in storitvah zaupanja (Uradni list RS, št. 121/21, 189/21 – ZDU-1M, 18/23 – ZDU-1O in 85/25).

(33) Izvajalec se zavezuje, da bo naročniku na njegovo pisno zahtevo omogočil izvajanje nadzorstva za upravljanje dostopa do informacijskih sistemov in informacij naročnika ter mu omogočil vpogled v notranje akte iz prejšnjega odstavka in ogled prostorov, v katerih se izvajajo pogodbena dela in hrani zaupna dokumentacija (najmanj enkrat letno), ter da bo upošteval naročnikove ugotovitve, zahteve, navodila in priporočila glede izvajanja posameznih varnostnih ukrepov iz te pogodbe.

(34) Naročnik se zavezuje, da bo pisno obvesti izvajalca najmanj dvajset dni pred predvidenim datumom izvedbe nadzora. Obvestilo mora vključevati opis področja pregleda, predviden potreben čas za izvedbo pregleda ter načrt virov, ki bodo na strani izvajalca potrebni za izvedbo pregleda. Nadzor se lahko izvaja v času rednega delovnega časa izvajalca oziroma podizvajalca. Javni uslužbenci naročnika, ki izvajajo nadzor, morajo podpisati izjavo o varstvu podatkov in upoštevati notranje akte izvajalca, ki urejajo informacijsko varnost pod pogojem, da bodo z njimi predhodno seznanjeni.

(35) Če izvajalec krši določbe te pogodbe, ki urejajo varovanje podatkov tudi po dodatnem roku, ki mu ga za izpolnitev določi naročnik, sme naročnik zahtevati razvezo te pogodbe in povrnitev škode.

(36) Pogodbena stranka, ki krši določbe o varovanju podatkov, je odškodninsko odgovorna za vso posredno in neposredno škodo po splošnih načelih obligacijskega prava.

(37) Pogodbena stranka lahko razkrije varovane podatke pristojnim nadzornim ali drugim državnim organom na način in pod pogoji, določenimi v področnem zakonu, ki ureja obveznost razkritja podatkov.

12. PROTIKORUPCIJSKA KLAVZULA

24. člen

Pogodbeni stranki potrjujeta, da sta seznanjeni z določbami 14. člena Zakona o integriteti in preprečevanju korupcije (Uradni list RS, št. 69/11 – uradno prečiščeno besedilo, 158/20, 3/22 – ZDeb in 16/23 – ZZPri; v nadaljnjem besedilu: ZIntPK; v nadaljnjem besedilu: ZIntPK) in se zavedata dejstva, da je ta pogodba nična, če je ali bo v katerikoli fazi sklepanja ali izvajanje te pogodbe kdo v imenu ali na račun druge pogodbene stranke, predstavniku ali posredniku naročnika ali organa ali organizacije iz javnega sektorja obljubil, ponudil ali dal kakšno nedovoljeno korist za pridobitev posla po tej pogodbi ali za sklenitev posla pod ugodnejšimi pogoji ali za opustitev dolžnega nadzora nad izvajanjem pogodbenih obveznosti ali za drugo ravnanje ali opustitev, s katerim je organu ali organizaciji iz javnega sektorja povzročena škoda ali je omogočena pridobitev nedovoljene koristi predstavniku organa, posredniku organa ali organizacije iz javnega sektorja, drugi pogodbeni stranki ali njenemu predstavniku, zastopniku, posredniku.

Pogodba je nična tudi v primeru, če izvajalec predloži lažno izjavo iz četrtega odstavka tega člena oziroma da neresnične podatke o navedenih dejstvih, skladno s šestim odstavkom 14. člena ZIntPK.

Naročnik bo v primeru ugotovitve o domnevnem obstoju dejanskega stanja iz prvega in drugega odstavka tega člena ali obvestila Komisije za preprečevanje korupcije ali drugih organov, glede njegovega domnevnega nastanka, pričel z ugotavljanjem pogojev ničnosti pogodbe iz prvega in drugega odstavka tega člena oziroma z drugimi ukrepi v skladu s predpisi Republike Slovenije.

Izjava izvajalca o udeležbi fizičnih in pravnih oseb v lastništvu izvajalca ter o povezanih družbah, ki je pridobljena skladno s šestim odstavkom 14. člena ZIntPK, je priloga __ k tej pogodbi. **Opomba UJP: obveznost predložitve izjave velja tudi za druge gospodarske subjekte (partnerje skupne ponudbe, podizvajalce), ki v zvezi s to pogodbo dobavljajo blago ali opravljajo storitve v vrednosti nad 10.000 EUR brez DDV.*

Naročnik nima zaposlenih funkcionarjev in posledično izvajalec ni dolžan predložiti izjave po 35. členu ZIntPK.

13. SKRBNIKA POGODBE

25. člen

Vsaka pogodbena stranka določi skrbnika te pogodbe.
Skrbnika nadzorujeta izvajanje pogodbe, razrešujeta morebitna nesoglasja, reklamacije, določata obliko in vsebino izvedbenih dokumentov (obrazci, poročila, zahteve, prijave, delovni nalogi, dobavnice, kontaktni podatki…) in podobno.
Podatki o skrbnikih pogodbe so priloga __ k tej pogodbi.

14. PREDČASNO PRENEHANJE POGODBE IN RAZVEZNI POGOJ

26. člen

Katerakoli od pogodbenih strank lahko zaradi kršitev pogodbenih obveznosti s strani nasprotne stranke, če kršitve ne prenehajo po pisnem opominu, odpove pogodbo z odpovednim rokom 30 dni od dneva vročitve odpovedi.

Odpoved pogodbe mora biti poslana v pisni obliki po pošti priporočeno s povratnico ali v elektronski obliki na e-naslov pogodbene stranke.

Ne glede na prejšnji odstavek in določbe Obligacijskega zakonika (Uradni list RS, št. 97/07 – uradno prečiščeno besedilo, 64/16 – odl. US in 20/18 – OROZ631) lahko naročnik predčasno odpove pogodbo z odpovednim rokom 30 dni od dneva vročitve odpovedi, brez kakršnekoli odškodninske odgovornosti do izvajalca, v primerih, ki so izrecno navedeni v posameznih členih te pogodbe ter tudi v naslednjih primerih:

- če nastanejo izredne okoliščine, na katere naročnik ni mogel vplivati in jih predvideti, zaradi katerih je postala izvedba javnega naročila nemogoča;
- če je pristojno sodišče izvajalcu izdalo sklep o začetku stečajnega postopka;
- če je izpolnjen najmanj pogoj iz 96. člena ZJN-3.

Izvajalec s podpisom ponudbe in te pogodbe potrjuje, da soglaša z možnostjo predčasnega prenehanja pogodbe, ter da se odpoveduje kakršnimkoli odškodninskim zahtevkom iz naslova zmanjšanja dohodka ali dobička ter drugim zahtevkom iz naslova zmanjšanja obsega naročila ali predčasnega prenehanja pogodbe, razen zahtevku za povračilo dejanskih stroškov, ki so mu nastali do prenehanja pogodbe (npr. za dejansko opravljene dobave blaga in storitve).

V primeru predčasnega prenehanja pogodbe sta pogodbeni stranki dolžni poravnati medsebojne pogodbene obveznosti, ki so bile realizirane in so dospele v plačilo do dneva prenehanja pogodbe.

27. člen

Ta pogodba je sklenjena pod razveznim pogojem, ki se uresniči v primeru izpolnitve ene od naslednjih okoliščin:

- če bo naročnik seznanjen, da je sodišče s pravnomočno odločitvijo ugotovilo kršitev obveznosti delovne, okoljske ali socialne zakonodaje s strani izvajalca;
- če bo naročnik seznanjen, da je pristojni državni organ pri izvajalcu ali podizvajalcu v času izvajanja pogodbe ugotovil najmanj dve kršitvi v zvezi s:
    - plačilom za delo,
    - delovnim časom,
    - počitki,
    - opravljanjem dela na podlagi pogodb civilnega prava kljub obstoju elementov delovnega razmerja ali
    - v zvezi z zaposlovanjem na črno

  in za kateri mu je bila s pravnomočno odločitvijo ali več pravnomočnimi odločitvami izrečena globa za prekršek.

V primeru seznanitve s kršitvijo bo naročnik o tem obvestil izvajalca v desetih dneh.

Izvajalec lahko v roku, ki ga bo določil naročnik, ki pa ne sme biti daljši kot 15 dni, predloži dokaze, da je sprejel zadostne ukrepe, s katerimi lahko dokaže svojo zanesljivost kljub obstoju kršitev. Če izvajalec ne bo predložil dokazov ali če jih bo, pa bo naročnik ocenil, da ti ukrepi ne zadoščajo, se razvezni pogoj uresniči pod pogojem, da je od seznanitve naročnika s kršitvijo in do izteka veljavnosti pogodbe še najmanj šest mesecev.

V primeru izpolnitve razveznega pogoja se šteje, da je pogodba za tega izvajalca razvezana z dnem sklenitve nove pogodbe o izvedbi javnega naročila za predmetno naročilo. O datumu sklenitve nove pogodbe bo naročnik obvestil izvajalca.

Če naročnik v 60 dneh od seznanitve s kršitvijo ne začne novega postopka javnega naročila, se šteje, da je pogodba razvezana šestdeseti dan od seznanitve s kršitvijo. **Opomba UJP: Če pogodbena dela izvajajo podizvajalci, se besedilo tega člena ustrezno dopolni, skladno z določbami 4. odstavka 67. člena ZJN-3.*

15. KONČNE DOLOČBE

28. člen

Pogodba se lahko spremeni v skladu s pogoji in okoliščinami, ki so opredeljene v 95. členu ZJN-3, ter zaradi drugih utemeljenih razlogov, ki ne smejo biti v nasprotju z določbami 95. člena ZJN-3.

Morebitne spremembe te pogodbe bosta pogodbeni stranki dopolnjevali pisno z aneksi k tej pogodbi.

V primeru, da ena od pogodbenih strank želi spremeniti pogodbo, je dolžna o tem pisno obvestiti drugo pogodbeno stranko ter ji posredovati predlog oziroma osnutek aneksa najmanj 10 dni vnaprej.

Za spremembo kontaktnih podatkov, navedenih v tej pogodbi in v prilogah k pogodbi, ter zamenjavo skrbnikov pogodbe in oseb, odgovornih za informacijsko varnost, je dovolj pisno obvestilo ene pogodbene stranke drugi pogodbeni stranki.

29. člen

Pogodbeni stranki se dogovorita, da bosta poskušali vse spore iz te pogodbe rešiti sporazumno z neposrednimi pogovori med pooblaščenimi predstavniki obeh pogodbenih strank. V kolikor sporazum med strankama ne bi bil mogoč, se dogovorita, da bo o sporih iz te pogodbe odločalo stvarno pristojno sodišče v Ljubljani.

30. člen

Glede medsebojnih pravic in obveznosti naročnika in izvajalca, ki niso urejene s to pogodbo, ali za tolmačenje pogodbe in presojo spornih vprašanj, se neposredno oziroma primarno uporabljajo določila razpisne dokumentacije ter določbe ZJN-3, Zakona o javnih financah, Zakona o izvrševanju proračuna Republike Slovenije in drugi predpisi, ki urejajo področje javnih financ in posebnosti poslovanja proračunskih uporabnikov, ter podrejeno (sekundarno) določbe Obligacijskega zakonika in drugih predpisov.

31. člen

Pogodba je napisana v 4 (štirih) enakih izvodih, od katerih prejme 3 (tri) izvode naročnik, 1 (en) izvod pa izvajalec. **Opomba UJP: Če bo pogodba podpisana elektronsko, se ta člen spremeni tako, da se glasi:*
»Ta pogodba je podpisana elektronsko s kvalificiranim elektronskim podpisom zastopnikov pogodbenih strank. Vsaka pogodbena stranka razpolaga z izvodom v elektronski obliki.«

32. člen

Pogodba začne veljati z dnem, ko jo podpišeta obe pogodbeni stranki, pod pogojem, da izvajalec naročniku izroči zahtevano finančno zavarovanje za dobro izvedbo pogodbenih obveznosti in odpravo napak v garancijskem roku v skladu s prvim odstavkom 22. člena te pogodbe.

Naročnik: **Izvajalec:**

Priloga št. __
k Pogodbi o dobavi, namestitvi, konfiguraciji in garancijskem vzdrževanju požarnih pregrad v komunikacijskem omrežju številka _____

Izjava podizvajalca

Podatki o podizvajalcu	
Ime in naslov podizvajalca *(ulica, hišna št., poštna št. in kraj):*	
Matična številka:	
Davčna številka:	
E-pošta:	
Telefon:	
Številka transakcijskega računa:	
Oseba, pooblaščena za zastopanje *(ime in priimek, funkcija):*	
Vrsta del, ki jih bo izvedel podizvajalec:	**predmet**: **količina**: **vrednost v EUR z DDV**: **kraj izvedbe**: **rok izvedbe**:

V zvezi s Pogodbo o dobavi, namestitvi, konfiguraciji in garancijskem vzdrževanju požarnih pregrad v komunikacijskem omrežju številka št. ____, nepreklicno izjavljamo *(ustrezno obkroži!)*:

- da pri izvajanju predmetnega javnega naročila **zahtevamo** neposredno plačilo s strani naročnika, ter da ta izjava velja kot naše soglasje po drugi alineji petega odstavka 94. člena Zakona o javnem naročanju (Uradni list RS, št. 91/15, 14/18, 121/21, 10/22, 74/22 – odl. US, 100/22 – ZNUZSZS, 28/23, 88/23 – ZOPNN-F in 83/25 - ZOUL; v nadaljnjem besedilu: ZJN-3), na podlagi katerega naročnik namesto ponudnika poravna naše terjatve do ponudnika neposredno nam;

- da pri izvajanju predmetnega javnega naročila **ne zahtevamo** neposrednega plačila s strani naročnika, ter da iz tega naslova nimamo do naročnika nobenih terjatev ali drugih zahtevkov.

Kraj: _____
Datum: _____

_____
(osebno ime, funkcija in lastnoročni ali elektronski podpis)

Priloga št. __
k Pogodbi o dobavi, namestitvi, konfiguraciji in garancijskem vzdrževanju požarnih pregrad v komunikacijskem omrežju številka _____

Izvajalec: _____
_____
_____
(ime in naslov)

V zvezi z izvajanjem Pogodbe o dobavi, namestitvi, konfiguraciji in garancijskem vzdrževanju požarnih pregrad v komunikacijskem omrežju številka _____, izjavljamo, da bodo storitve izvajali naslednji kadri:

Zap. št.	Ime in priimek	Naziv delovnega mesta	Opis nalog pri izvedbi tega javnega naročila

Kraj: _____

Datum: _____

Žig
(če ga izvajalec uporablja)

Podpisnik:

_____
(osebno ime, funkcija in lastnoročni ali elektronski podpis)

Priloga št. __
k Pogodbi o dobavi, namestitvi, konfiguraciji in garancijskem vzdrževanju požarnih pregrad v komunikacijskem omrežju številka (v nadaljnjem besedilu: Pogodba št. _____), ki sta jo sklenila Uprava Republike Slovenije za javna plačila, Dunajska cesta 48, 1000 Ljubljana (v nadaljnjem besedilu: **naročnik** ali **UJP**), in _____ (v nadaljnjem besedilu: **izvajalec**).

IZJAVA O VARSTVU PODATKOV

1. Podatki o delavcu in delodajalcu:

Delavec:	
Delodajalec:	

2. Obveznost varovanja zaupnih podatkov, pridobljenih pri izvajanju javnega naročila:

V zvezi z varovanjem poslovne skrivnosti, uradne skrivnosti, tajnih podatkov, davčne tajnosti, osebnih podatkov in drugih varovanih podatkov (v nadaljnjem besedilu: zaupni podatki), ki mi bodo razkriti oziroma dostopni pri izvajanju delovnih nalog po Pogodbi _____,

izjavljam,

- da bom zaupne podatke obdeloval izključno v dovoljene namene in le v dovoljenem obsegu, ki je potreben za opravljanje mojih delovnih nalog po Pogodbi _____;
- da zaupnih podatkov v času trajanja delovnega ali drugega pogodbenega razmerja pri izvajalcu niti kadarkoli po prenehanju razmerja, ne bom prisvojil, kopiral ali izkoriščal za svojo osebno uporabo ali omogočil, da bi jih uporabljale tretje osebe ali razkril tretjim osebam, razen v primerih, določenih z zakonom;
- da se bom pri izvajanju delovnih obveznosti po Pogodbi _____ vzdržal vseh ravnanj, ki lahko moralno ali materialno škodujejo ali bi lahko škodovala interesom naročnika (UJP);
- da bom z varovanimi podatki, s katerimi bom prišel v stik pri izvajanju pogodbenih del, ravnal v skladu z veljavnimi zakonskimi in podzakonskimi predpisi, ki urejajo varovanje poslovne skrivnosti, tajnih podatkov, davčne tajnosti, osebnih podatkov in informacijske varnosti, ter z notranjimi akti delodajalca / izvajalca, ki urejajo postopke, organizacijske in tehnične ukrepe za varovanje podatkov, komunikacijske opreme, strojne in sistemske aplikativne programske opreme ter poslovnih prostorov;
- da mi je delodajalec (izvajalec / podizvajalec) pred nastopom dela omogočil seznanitev s predpisi in notranjimi akti iz prejšnje alineje;
- da bom v primeru izvedbe pogodbenih del na lokaciji naročnika (UJP) pri delu in gibanju v prostorih upošteval njegova varnostna pravila pod pogojem, da bom z njimi predhodno seznanjen ob vstopu v varovane prostore;
- da s svojimi dejanji in aktivnostmi ne bom ogrožal razpoložljivosti in neoporečnosti virov informacijskega sistema naročnika (UJP);
- da se zavedam vseh posledic (delovno-pravnih, odškodninskih, prekrškovnih, kazenskih) v primeru kršitve dolžnosti varovanja podatkov, ki so določene z veljavnimi predpisi, ki urejajo delovna razmerja, obligacijska razmerja, varstvo zaupnih podatkov, informacijsko varnost in odgovornost za kazniva dejanja.

Datum: ---------- ----------

(lastnoročni ali elektronski podpis)

Priloga št. __
k Pogodbi o dobavi, namestitvi, konfiguraciji in garancijskem vzdrževanju požarnih pregrad v komunikacijskem omrežju številka _____

PODATKI O SKRBNIKIH POGODBE

Skrbnik pogodbe na strani UJP:	Osebno ime:	
	Telefon:	
	E-pošta:	

Skrbnik pogodbe na strani izvajalca:	Osebno ime:	
	Telefon:	
	E-pošta:	

PODATKI O OSEBAH, ODGOVORNIH ZA INFORMACIJSKO VARNOST

Pooblaščena oseba na strani UJP:	Osebno ime:	
	Telefon:	
	E-pošta:	

Pooblaščena oseba na strani izvajalca:	Osebno ime:	
	Telefon:	
	E-pošta:	

Priloga št. __
k Pogodbi o dobavi, namestitvi, konfiguraciji in garancijskem vzdrževanju požarnih pregrad v komunikacijskem omrežju številka številka _____

Izjava o lastništvu in povezanih družbah

Izvajalec: _____

(ime in naslov, matična in davčna številka)

Na podlagi 6. odstavka 14. člena Zakona o integriteti in preprečevanju korupcije (Uradni list RS, št. 69/11 – uradno prečiščeno besedilo, 158/20, 3/22 – ZDeb in 16/23 - ZZPri; v nadaljnjem besedilu: ZIntPK) zaradi zagotovitve transparentnosti posla in preprečitve korupcijskih tveganj pri izvajanju javnega naročila oziroma Pogodbe o dobavi, namestitvi, konfiguraciji in garancijskem vzdrževanju požarnih pregrad v komunikacijskem omrežju številka št. _____

IZJAVLJAMO:

a) da so v lastništvu izvajalca udeležene naslednje osebe:

Zap. št.	*Firma pravne osebe oziroma ime in priimek fizične osebe, ki je posredno ali neposredno imetnik več kakor 5 % delnic oziroma je udeležena z več kot 5 % ustanoviteljskim deležem*	*Poslovni naslov pravne osebe oziroma naslov prebivališča fizične osebe*	*Osnovni vložek v EUR*	*Delež lastništva v odstotku (%)*
Opomba UJP: v primeru večjega števila družbenikov se obrazec ustrezno dopolni (v Word formatu) ali pa se priloži izpisek iz sodnega registra ali drug verodostojen dokument, iz katerega morajo biti razvidni vsi zgoraj zahtevani podatki.				

b) da se v skladu z določbami 527. do 562. člena Zakona o gospodarskih družbah (Uradni list RS, št. 65/09-UPB3 s spremembami in dopolnitvami; v nadaljnjem besedilu: ZGD-1) šteje, da je izvajalec povezan z naslednjimi gospodarskimi subjekti (povezane družbe):

Zap. št.	*Firma pravne osebe*	*Poslovni naslov pravne osebe*	*Matična številka ali druga identifikacijska oznaka pravne osebe*	*Vrsta (opis) razmerja po 527. členu ZGD-1*
Opomba UJP: v primeru večjega števila gospodarskih družb se obrazec ustrezno dopolni (v Word formatu) ali pa se priloži izpisek iz sodnega registra ali drug verodostojen dokument, iz katerega morajo biti razvidni vsi zgoraj zahtevani podatki.				

Izjavljamo, da smo kot fizične osebe - udeležence v lastništvu izvajalca navedli:

- vsako fizično osebo, ki je posredno ali neposredno imetnik več kakor 5% delnic, oziroma je udeležena z več kot 5% deležem pri ustanoviteljskih pravicah, upravljanju ali kapitalu pravne osebe, ali ima obvladujoč položaj pri upravljanju sredstev pravne osebe;
- vsako fizično osebo, ki pravni osebi posredno zagotovi ali zagotavlja sredstva, in ima na tej podlagi možnost nadzorovati, usmerjati ali drugače bistveno vplivati na odločitve uprave ali drugega poslovodnega organa pravne osebe pri odločanju o financiranju in poslovanju.

S podpisom te izjave jamčimo, da v celotni lastniški strukturi izvajalca ni udeleženih drugih fizičnih ali pravnih oseb ter gospodarskih subjektov, za katere se glede na določbe ZGD-1 šteje, da so povezane družbe.

Zagotavljamo, da so podatki v tej izjavi resnični, popolni in točni ter se zavezujemo, da bomo naročnika takoj obvestili o vsaki spremembi zgoraj navedenih podatkov.

Seznanjeni smo s šestim odstavkom 14. člena ZIntPK, ki določa, da predložitev lažne izjave oziroma navedba neresničnih podatkov, ima za posledico ničnost pogodbe.

Kraj:

Datum: ___

_____

(osebno ime, funkcija in lastnoročni ali elektronski podpis)

**Opomba UJP: obveznost predložitve izjave velja tudi za druge gospodarske subjekte (partnerje skupne ponudbe, podizvajalce), ki pri izvedbi predmetnega javnega naročila opravljajo dobave opreme in storitve v vrednosti nad 10.000 EUR brez DDV.*

Priloga št. __
k Pogodbi o dobavi, namestitvi, konfiguraciji in garancijskem vzdrževanju požarnih pregrad v komunikacijskem omrežju številka _____

MENIČNA IZJAVA S POOBLASTILOM ZA IZPOLNITEV

Izvajalec (izdajatelj menice / trasant):

Firma:	
Poslovni naslov:	
Davčna številka:	
Matična številka:	

(v nadaljnjem besedilu: **izvajalec**)

V skladu z 18. členom Pogodbe o dobavi, namestitvi, konfiguraciji in garancijskem vzdrževanju požarnih pregrad v komunikacijskem omrežju številka _____(v nadaljnjem besedilu: pogodba), ki sklenjena med izvajalcem in naročnikom: Republika Slovenija, Ministrstvo za finance, Uprava Republike Slovenije za javna plačila, Dunajska cesta 48, 1000 Ljubljana, davčna številka 10641424, matična številka 1572814, šifra proračunskega uporabnika 16187 (v nadaljnjem besedilu: UJP ali naročnik ali menični upnik), za zavarovanje vseh naših obveznosti iz navedene pogodbe naročniku izročamo tri (3) bianco menice, ki jih je podpisal_____.

S podpisom te izjave izvajalec nepreklicno pooblašča naročnika (UJP), da v primeru kršitve ali neizpolnitve pogodbenih obveznosti, kot je opredeljeno v 22. členu navedene pogodbe, unovči menično zavarovanje, pri čemer naročnik izpolni vse ostale sestavine posamezne bianco menice, ki ob izdaji niso bile izpolnjene, kot sledi:

- **kraj in datum izdaje:** je sedež dobavitelja / izvajalca (izdajatelja menice) in datum podpisa te izjave;
- **znesek s številko in znesek z besedo:** je znesek v EUR, ki ga vpiše naročnik, pri čemer menični znesek na posamezni menici oziroma kumulativni znesek vseh menic, posredovanih na unovčenje na podlagi te menične izjave, ne sme biti višji od zneska _____ EUR (10 % skupne pogodbene vrednosti z DDV);
- **dospelost plačila:** vpiše se dospelost na določen dan, ki ga poljubno izbere naročnik kadar koli po kršitvi pogodbenih obveznosti oziroma ob izpolnitvi pogojev za unovčenje menice, določenih v 22. členu pogodbe, vendar najpozneje 30 dni po prenehanju pogodbe; po izteku tega roka menica ne sme biti predložena na unovčenje;
- **klavzula »plačajte za to…...menico«**: ta klavzula se lahko prečrta in nadomesti s klavzulo »bomo plačali to menico«;
- **po nalogu (ime remitenta)**: tu se vpiše menični upnik – Republika Slovenija, Ministrstvo za finance, Uprava Republike Slovenije za javna plačila;
- na menici lahko naročnik vpiše klavzule: »brez protesta«, »brez obvestila«, »plačljivo na prvi poziv«;
- **plačljivo pri:** naročnik lahko vpiše kateregakoli ponudnika plačilnih storitev, s sedežem v Republiki Sloveniji, pri katerem ima dobavitelj / izvajalec (izdajatelj menice - trasant) odprt transakcijski račun, in sicer:
    - _____,
    - _____,
    - ali na katerem koli drugem transakcijskem računu dobavitelja / izvajalca, odprtem pri kateremkoli ponudniku plačilnih storitev, s sedežem v Republiki Sloveniji (v nadaljnjem besedilu: banka – domiciliat), ki je evidentiran v Poslovnem registru

Slovenije oziroma Registru transakcijskih računov, tako v času podpisa te menične izjave kot v času unovčenja posamezne menice.

S podpisom te menične izjave / pooblastila soglašamo, da posamezna bianco menica po izpolnitvi zgoraj navedenih meničnih sestavin velja in se uporablja kot domicilirana menica. Naročnik, kot imetnik domicilirane menice, lahko poljubno pripravi, izpolni in podpiše plačilni nalog ter odredi izvršitev plačilnega naloga oziroma plačilne transakcije na podlagi domicilirane menice v skladu z določbami 186. in 187. člena Zakona o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (Uradni list RS, št. 7/18, s spremembami in dopolnitvami; v nadaljnjem besedilu: ZPlaSSIED). Menični znesek se nakaže naročniku na račun Republike Slovenije št. IBAN SI56 0110 0630 0109 972, s sklicem oziroma referenco, ki jo določi naročnik.

Za podpisano domicilirano menico se šteje, da vključuje nepreklicno dobaviteljevo / izvajalčevo pooblastilo naročniku (imetniku menice), da odredi izvršitev plačilnega naloga oziroma plačilne transakcije v breme izvajalčevih računov, in hkrati soglasje banki – domiciliatu, da v breme izvajalčevih denarnih sredstev izvrši plačilni nalog oziroma plačilno transakcijo, ki jo odredi (naročnik) imetnik menice v skladu z določbami 186. in 187. člena ZPlaSSIED.

S podpisom tega pooblastila in menične izjave nepreklicno in brezpogojno pooblaščamo vsako banko – domiciliata, ki vodi naš transakcijski račun:

- da v skladu s 1. točko tretjega odstavka 240. člena ZPlaSSIED naročniku (UJP) razkrije podatke, potrebne za unovčenje posamezne menice;
- da iz našega dobroimetja na transakcijskem računu izplača vsako domicilirano menico, ki jo predloži v plačilo naročnik – UJP;
- da izvrši konverzijo iz razpoložljivih tujih valut v EUR, če je/bo naš račun voden v več tujih valutah in če ne bo dovolj sredstev za unovčenje menice v domači valuti (EUR).

Nepreklicno izjavljamo, da naročniku (UJP) posamezne menice ni treba protestirati, da se odrekamo vsem ugovorom proti meničnim plačilnim nalogom oziroma sklepu o izvršbi na podlagi menice in da bomo naročniku poravnali vso nastalo škodo zaradi neizvršitve oziroma nepravilne izvršitve plačila menice, domicilirane pri kateri koli banki, ki vodi naš transakcijski račun.

Naročnik mora menico, če jo ne bo uporabil v zgoraj navedene namene, vrniti izvajalcu v 60 dneh po prenehanju veljavnosti pogodbe.

Podpisane menice in menična izjava veljajo tudi v primeru spremembe zastopnika/ov izvajalca oziroma podpisnika/ov te izjave in menic.

Ta menična izjava velja od dneva podpisa in še 30 dni po prenehanju pogodbe.

Kraj: _____

Datum: _____

Izvajalec:

_____

(lastnoročni ali elektronski podpis)

Priloga:

- 3 bianco menice, potrjene z žigom izvajalca in lastnoročnim podpisom zakonitega zastopnika

III. PONUDBENA DOKUMENTACIJA

Obrazec 2 – Ponudba / Predračun

Ponudnik: _____

(ime in naslov)

Št. ponudbe: _____

(evidenčna številka ponudnika)

PONUDBA / PREDRAČUN

V skladu z razpisno dokumentacijo za javno naročilo *»Dobava, namestitev, konfiguracija in garancijsko vzdrževanje požarnih pregrad v komunikacijskem omrežju«, z oznako 4/2026-JNMV-PP,* naročniku ponujamo dobavo opreme in izvedbo storitev po naslednji specifikaciji:

Zap. št.	Predmet ponudbe	Ponujeni proizvajalec, tip/model oziroma oznaka	Enota mere	Količina	Cena na enoto brez DDV (EUR)	Skupna vrednost brez DDV (EUR)
1.1	Požarna pregrada Palo Alto Networks PA-560 ali enakovredna, skladna s tehničnimi zahtevami naročnika		kos	2		
1.2	Naročnina Precision AI Network Security Subscription Bundle za PA-560, ki vključuje Advanced Threat Prevention in Advanced URL Filtering, ali enakovredna naročnina za obdobje treh (3) let		kos	2		
1.3	Napajalnik 150 W za PA-560 ali enakovreden za zagotavljanje redundantnega napajanja		kos	2		
1.4	Komplet 10G SFP+ modulov in povezovalnih optičnih kablov dolžine 5m *(1 komplet = 2xSFP+ modul in 1x povezovalni kabel)*		komplet	8		
1.5	Storitve dobave, namestitve, konfiguracije, migracije, testiranja in primopredaje rešitve		komplet	1		
1.6	Vzdrževanje, tehnična podpora v režimu 24x7 in dostop do posodobitev za celotno rešitev za obdobje treh (3) let		komplet /mesec	36 mesecev	*0,00	*0,00
Skupna ponudbena vrednost brez DDV (EUR)						
DDV 22 % (EUR)						
Skupna ponudbena vrednost z DDV (EUR)						

*Garancijsko vzdrževanje je brezplačno oziroma všteto v kupnino/ceno opreme.

DDV se obračuna po veljavni davčni stopnji.

V ceno brez DDV so vključeni naslednji stroški:
- kupnina za dva kompleta požarnih pregrad (vključno s pripadajočo opremo),
- kupnina za licence,
- storitve, povezane z namestitvijo in konfiguracijo opreme,
- vzdrževanje strojne opreme,
- cena delovne ure serviserja, pripravljenost, potni stroški, čas servisiranja itd.,
- zagotavljanje odzivnega časa in popravila v zahtevanem režimu vzdrževanja,

- stroški rezervnih delov in nadomestne računalniške opreme,
- stroški potrošnega materiala in medijev potrebnih za izvedbo vzdrževanja,
- stroški skladiščenja priporočenih rezervnih delov in opreme, ki omogoča zamenjavo v zahtevanem režimu,
- tehnična podpora za licenčno programsko opremo,
- stroški, povezani z nadgradnjo in novimi verzijami programske opreme,
- sistemsko konfiguriranje,
- pomoč po telefonu,
- usposabljanje uporabnikov računalniške opreme, zaposlenih pri naročniku,
- zagotavljanje uporabniške dokumentacije,
- zagotavljanje garancij za rezervne dele, opremo in opravljene storitve,
- stroški, povezani z zagotavljanjem ustreznih finančnih zavarovanj za dobro izvedbo pogodbenih obveznosti in odpravo napak v garancijskem roku, skladno z vzorcem pogodbe, ki je sestavni del razpisne dokumentacije,
- drugi stroški, ki se neposredno ali posredno nanašajo na dobavo, namestitev, konfiguracijo in vzdrževanje opreme.

Cene blaga in storitev, izražene v EUR brez DDV, so fiksne.

Oprema in storitve se obračunavajo v skladu s plačilnimi pogoji, ki so opredeljeni v vzorcu pogodbe, ki je sestavni del razpisne dokumentacije.

Soglašamo s pogoji finančnega zavarovanja, določenimi v vzorcu pogodbe in razpisni dokumentaciji. V primeru, da bomo izbrani na predmetnem javnem naročilu, bomo naročniku v roku osmih (8) dni po podpisu pogodbe zagotovili 3 menice in menično izjavo v višini 10 % celotne pogodbene vrednosti z DDV, veljavno od dneva izdaje in najmanj 30 dni po prenehanju pogodbe, skladno z vzorcem iz razpisne dokumentacije.

Ponudba / predračun velja najmanj 3 mesece od dneva oddaje prek informacijskega sistema e-JN.

V_____, dne .....

.....

*(lastnoročni ali elektronski podpis; *žig ni obvezen, če je dokument podpisan elektronsko)*

Navodilo UJP:
V primeru skupne ponudbe obrazec izpolni in podpiše vodilni oziroma poslovodeči partner poslovne skupine ali konzorcija.

Uporaba žiga na dokumentu ni potrebna, če je dokument podpisan z varnim digitalnim podpisom, overjenim s kvalificiranim digitalnim potrdilom, ali če ponudnik v skladu z notranjimi akti žiga ne uporablja.

Izpolnjen obrazec v PDF datoteki ponudnik v informacijskem sistemu e-JN pripne oziroma naloži v razdelek »Predračun« tako, da bo obrazec razkrit/dostopen na javnem odpiranju ponudb.

Obrazec 3 – Izjava o tehnični in funkcionalni skladnosti ponujene opreme in storitev

Ponudnik: _____

_____

_____

(ime in naslov)

IZJAVA
O TEHNIČNI IN FUNKCIONALNI SKLADNOSTI PONUJENE OPREME IN STORITEV

Naročniku zagotavljamo, da ponujena kompleta požarnih pregrad in storitve ustrezajo vsem splošnim in tehničnim zahtevam iz razpisne dokumentacije, opisanim v nadaljevanju.

1. Splošne zahteve

Oprema omogoča oddaljeni dostop za 150 uporabnikov naročnika (RAVPN).

Ponujena oprema je funkcionalno in protokolno združljiva z obstoječim komunikacijskim omrežjem naročnika, tehnično preverjena ter mora zagotavljati zanesljivo delovanje v obstoječem sistemu oziroma omrežju.

Oprema je skladna z zahtevano konfiguracijo, namenjena slovenskemu trgu ter opremljena z vsemi potrebnimi veljavnimi atesti in dovoljenji za uporabo v Republiki Sloveniji. Omogoča uporabo in vzdrževanje v Sloveniji brez dodatnih prilagoditev ali sprememb.

Vsa strojna oprema je nova in proizvedena v letu 2026.

Ponudnik je pooblaščen serviser ponujene opreme ter zagotavlja rezervne dele za vso ponujeno opremo v zahtevani konfiguraciji najmanj pet (5) let od dneva primopredaje opreme.

2. Tehnične zahteve in lastnosti obeh požarnih pregrad

Navedene lastnosti in zmogljivosti veljajo za dve požarni pregradi:

2.1. Splošne lastnosti:

1. požarna pregrada omogoča aplikacijsko pregledovanje in nadziranje prometa (angl. NGFW požarna pregrada),
2. požarna pregrada ima zasnovo primerno za okolja z visoko zanesljivostjo (active/passive HA),
3. požarna pregrada je namenska naprava (ne gre za virtualno napravo),
4. proizvajalec požarne pregrade se nahaja v četrtem (leader) kvadrantu Gartner poročil za Next-Generation požarne pregrade vsaj zadnjih 5 let,
5. postavitev požarne pregrade omogoča naslednje scenarije:
   - transparentni prehod za prestrezanje (Virtual Wire),
   - L3 način (požarna pregrada je privzeti prehod napravam v omrežju),
   - zajem kopije prometa za analizo (tap),
   - L2 način,
6. požarna pregrada ima fizično ločeno upravljalno ravnino (angl. Management plane), ki skrbi za grafični vmesnik in konfiguracijo, ter podatkovno ravnino (angl. Data plane), ki obravnava promet, ki poteka skozi požarno pregrado. Poleg tega ima požarna pregrada najmanj 2 CPU jedri, namenjeni izključno upravljalni ravnini,
7. požarna pregrada ima fizično ločen upravljalni vmesnik (out-of-band management), ki omogoča popolno izolacijo upravljanja od produkcijskega prometa.

2.2. Tehnične zmogljivosti:

1. požarna pregrada je strojna, namenska naprava, optimizirana z ustreznimi pospeševalnimi komponentami (npr. ASIC, FPGA), tako da vse NGFW storitve izvaja pospešeno na namenski strojni opremi; poizvedbe na upravljalni ravnini pri tem ne vplivajo na pretočni oziroma podatkovni del,
2. požarna pregrada omogoča vsaj 8,5 Gbps prepustnosti pri aplikacijskem pregledovanju in nadzoru vsega prometa,
3. požarna pregrada mora omogoča vsaj 6 Gbps prepustnosti pri aplikacijskem pregledovanju in nadzoru vsega prometa ter pri vključenih vseh varnostnih preverjanjih prometa (angl. Threat Prevention Throughput). Navedena zahteva se ne nanaša zgolj na prepustnost pri varnostnih preverjanjih, ki so predmet tega naročila, temveč je zagotovljena tudi ob morebitnem kasnejšem dodajanju novih varnostnih preverjanj,
4. požarna pregrada omogoča vsaj 5,5 Gbps prepustnosti pri prometu IPSec VPN, najmanj 598.000 sočasnih sej, najmanj 100.000 novih sej na sekundo ter najmanj 10 virtualnih usmerjevalnikov (npr. VRF),
5. požarna pregrada podpira virtualizacijo oziroma razdelitev na najmanj pet (5) virtualnih razdelkov z neodvisnimi vmesniki in politikami ter že vključuje možnost uporabe vsaj enega (1) virtualnega razdelka (virtualni sistemi, konteksti),
6. požarna pregrada ima vgrajena dva (2) napajalnika za zagotavljanje podvojenosti, z možnostjo menjave med delovanjem,
7. požarna pregrada je primerna za montažo v strežniško omaro oziroma bo priložen ustrezen komplet za montažo v strežniško omaro (angl. rack mountable), višine 1RU in širine 19 palcev.

2.3. Podpora vmesnikom na napravi:

- vsaj 4 x SFP (1 Gbps),
- vsaj 4 x SFP+ (10 Gbps),
- vsaj 16 x RJ45 (10Mbps/100Mbps/1Gbps),
- vsaj 1 Gbps (RJ45) port namenjen ločenemu upravljanju naprave.

2.4. Funkcionalne lastnosti:

1. aplikacijsko preverjanje in nadziranje prometa se vedno izvaja na vsem prometu, ki gre skozi požarno pregrado, ne glede na port ali protokol,
2. požarna pregrada podpira aplikacijsko bazo z več kot 5000 aplikacijami z dinamičnimi filtri na podlagi naslednjih kriterijev: kategorija, podkategorija, vedenjske značilnosti, osnovna tehnologija ali dejavnik tveganja,
3. požarna pregrada omogoča zaznavanje in obravnavo neznanih in prej nevidenih groženj na osnovi strojnega učenja in vedenjske analize,
4. požarna pregrada omogoča naknadno prepoznavo in klasifikacijo neznanega prometa s posebej napisanimi pravili ali signaturami,
5. požarna pregrada omogoča zaščito pred znanimi ranljivosti (IPS), poleg zaščite na osnovi signatur omogoča tudi dodatno zaščito pred neznanimi in zero-day napadi v realnem času (inline) z uporabo strojnega učenja in globokega učenja v oblaku proizvajalca naprave,
6. požarna pregrada lahko analizira šifrirani prometa z uporabo TLS finger-printinga tudi brez popolne dešifriranosti vsebine,
7. požarna pregrada omogoča blokiranje škodljive programske kode (angl. Antivirus),
8. požarna pregrada zagotavlja algoritme strojnega učenja (angl. Machine Learning) za napredno zaščito na sami napravi. S tem omogoča hitro, lokalno analizo zero-day groženj in drugih izmikajočih se napadov na osnovi strojnega učenja, pri čemer niso potrebne zunanje povezave. Požarna pregrada podpira analizo Zero-Day zlonamerne programske opreme brez uporabe signatur (za zaznavanje izmikajočega se in neznanega prometa, kot je C2, za zaznavanje orodij, kot sta Cobalt Strike in Empire, proti napadom z vbrizgavanjem

ukazov in SQL vbrizgavanjem) in mora podpirati naslednje protokole: HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP in SMB,

9. požarna pregrada ima podporo za IPS podpise za zaznavanje post-kvantnih algoritmov in napadi zmogljivih kvantnih računalnikov (angl. Post Quantum Cyphers),
10. požarna pregrada omogoča zaščito pred 0-day napadi; rešitev vključuje mehanizme za proaktivno zaznavanje in preprečevanje neznanih groženj (0-day), kot so vedenjska analiza prometa, strojno učenje, detekcija anomalij ter integracija z globalnimi bazami groženj v realnem času,
11. požarna pregrada omogoča zaščito pred 0-day napadi s tem da omogoča pošiljanje datotek v analizo v izolirano okolje proizvajalca (angl. Cloud sandbox),
12. v primeru, da proizvajalec požarne pregrade odkrije novo škodljivo kodo in izda ustrezno zaščito, požarna pregrada to zaščito prejme takoj (posodabljanje v realnem času),
13. požarna pregrada omogoča prepoznavo morebitnih že okuženih naprav v omrežju (anti-bot, antispyware), poleg zaščite na osnovi signatur omogoča tudi dodatno preverjanje sumljivega prometa v realnem času v oblaku proizvajalca naprave,
14. požarna pregrada omogoča prepoznavo, spremljanje in blokiranje različnih datotek (izvedljive datoteke, PDF dokumenti MS office dokumenti…) v poljubni smeri (upload ali download),
15. požarna pregrada privzeto podpira tudi skeniranje izvedljivih datotek za macOS in Linux. V tem smislu rešitev zagotavlja podrobno analizo vsake analizirane datoteke na več operacijskih sistemih, vključno z informacijami o dejavnosti na ravni naprave in omrežja. Omogoča tudi dostop do izvirne datoteke, vključno s PCAP z dinamično analizo seje, če je datoteka obravnavana kot zlonamerna programska oprema za obratni inženiring, ter podrobno poročilo v PDF-u s statično in dinamično analizo,
16. požarna pregrada omogoča vključitev katere koli nove varnostne funkcije, ne da bi to vplivalo na zmogljivost prometa, ki poteka skozi njo. To pomeni, da že v osnovi nuditi vsaj kontrolo aplikacij, IPS, protivirusno zaščito, antispyware, sandboxing, blokiranje datotek, URL filtriranje, DNS zaščito in beleženje dogodkov,
17. požarna pregrada omogoča možnost zahtevanja URL re-kategorizacije znotraj grafičnega vmesnika požarne pregrade,
18. požarna pregrada podpira varnostne politike z uporabo explicit proxy funkcionalnosti,
19. požarna pregrada podpira možnost ustvarjanja varnostnih politik za preprečevanje kraje poverilnic in preprečevanje uhajanja korporativnih poverilnic na spletne strani tretjih oseb. Pri tem se mora za preverjanje poverilnic uporabiti Bloom filter,
20. požarna pregrada dinamično analizira URL-je v realnem času tudi za sveže generirane URL-je, domene brez zgodovine ter neznane oz. neklasificirane URL-je,
21. požarna pregrada dinamično v realnem času analizira in blokira dostop do sofisticiranih še nikoli videnih strani lažnega predstavljanja (phishing strani) z uporabo naprednih detekcijskih anti-phishing mehanizmov, ki so osnovani na algoritmih globokega učenja,
22. požarna pregrada podpira zaščito DNS varnosti, kot so: zaznavanje DNS povratnih klicev domen (škodljiva programska oprema in C2 domene, Botnet domene, Fast-flux domene, naključni DGA, dictionary DGA), DNS domen z visokim tveganjem (grayware, novo registrirane domene, parkirane domene, izogibanje proxyjem, dinamični DNS, napovedno zaznavanje, strateško stare domene), napadov na DNS zapise (Domain squatting, dangling DNS, kompromitirana DNS cona, Wildcard DNS, CNAME cloaking), napadov na DNS protokol (DNS Rebinding, NXNS napadi), zaznavanje DNS tuneliranja, ultra-počasno DNS tuneliranje in DNS infiltracije, ter podporo za DNS sinkholing za identifikacijo okuženih naprav v omrežju,
23. Anti-Virus in URL filtriranje podpisov in vsebina sta avtorsko delo proizvajalca požarne pregrade (tj. nobena tretja stranka za A/V ali URL filtriranje podpisov),
24. požarna pregrada je sposobna dešifrirati TLS v1.3 seje z uporabo zunanjih Hardware Security Modules (HSM) za shranjevanje zasebnih ključev,

25. požarna pregrada omogoča ustvarjanje kopije dešifriranega prometa iz požarne pregrade (angl. Decryption mirroring) in njeno pošiljanje orodjem za zbiranje prometa za forenziko, zgodovinske namene ali preprečevanje izgube podatkov (DLP),
26. požarna pregrada podpira IPS, zaščito pred zlonamerno programsko opremo, filtriranje vsebine in URL filtriranje v enem samem varnostnem pravilu,
27. požarna pregrada omogočati dešifriranje SSL/HTTPS in SSH prometa,
28. SSL inspekcija je sposobna v celoti izpolnjevati TLS 1.2 visoke / srednje šifrirne algoritme in ne sme prekiniti pogajanja o TLS 1.3,
29. požarna pregrada omogoča spremljanje in uporabo zunanjih dinamičnih seznamov IP naslovov, domen in URL naslovov (integracija z obstoječimi sistemi za zaznavo anomalij v omrežju),
30. požarna pregrada omogoča filtriranje spletnih strani na osnovi kategorij ali specifičnih URL naslovov. Administrator poleg tega lahko ustvari in uporablja lastne kategorije in specifične URL naslove v pravilih, ne da bi imel pri tem kakršnekoli omejitve,
31. požarna pregrada omogoča samodejno odkrivanje in identifikacija vseh naprav v omrežju (IT, IoT, OT, IoMT, BYOD) brez uporabe agentov,
32. požarna pregrada pripisuje naslednje lastnosti napravam: tip, proizvajalec, model, operacijski sistem in raven tveganja,
33. požarna pregrada dinamično uveljavlja Zero-Trust varnostnih politik glede na kontekst in tveganje naprave,
34. požarna pregrada ima integrirano vidljivost, ocenjevanje tveganj in prioritetna obravnava ranljivosti prepoznanih naprav v omrežju,
35. požarna pregrada lahko agregira SD-WAN povezave oddaljenih lokacij (Hub), ter omogoča aplikacijsko zavedno usmerjanje prometa glede na zakasnitev, izgubo paketov in jitter,
36. požarna pregrada lahko samodejno preusmerjanje prometa brez prekinitve seje (sub-second failover),
37. požarna pregrada omogoča hiter vpogled v promet preko požarne pregrade za obdobje zadnjih nekaj ur ali dni, analiziran glede na aplikacijo, izvorni IP naslov ali ciljni IP naslov,
38. požarna pregrada omogoča avtomatično izdelavo in hranjenje obdobnih poročil o aplikacijah, prometu in varnostnih dogodkih,
39. požarna pregrada omogoča izdelavo lastnih obdobnih poročil glede na poljubne kriterije ali filtre,
40. požarna pregrada omogoča izvoz poročil in pošiljanje preko e-pošte,
41. požarna pregrada omogoča zaznavo uporabljenih in ne uporabljenih pravil zaradi optimizacije delovanja,
42. požarna pregrada omogoča beleženje vseh aplikacij, ki so bile dovoljene po posameznem pravilu (za prehod v aplikacijsko politiko), ter količino prometa za posamezno aplikacijo dovoljenega po tem pravilu,
43. požarna pregrada omogoča integracijo s poljubnim LDAP strežnikom za pridobivanje informacij o uporabnikih in uporabniških skupinah,
44. požarna pregrada omogoča prepoznavo uporabnikov preko portalov za identifikacijo (angl. Captive portal),
45. požarna pregrada omogoča prepoznavo uporabnikov iz drugih sistemov na podlagi syslog sporočil,
46. požarna pregrada omogoča pisanje varnostne politike glede na uporabnike in uporabniške skupine,
47. požarna pregrada omogoča vpeljavo dodatnega overjanja tudi z uporabo MFA za dostop do najbolj kritičnih sistemov oziroma strežnikov,
48. požarna pregrada omogoča izvoz logov preko syslog formatov BSD, IETF ali poljubno definirane oblike (za integracijo s SIEM in ostalimi sistemi),
49. požarna pregrada omogoča natančno filtriranje logov pri izvozu preko syslog formata glede na vrsto loga, resnost dogodka, tip dogodka, kategorijo dogodka, pravilo (za integracijo s SIEM in ostalimi sistemi),

50. požarna pregrada omogoča preprost pregled vseh dogodkov v realnem času z možnostjo filtriranja prometa vsaj po naslednjih parametrih (izvor prometa, cilj prometa, protokol, ciljni port, izvorni port, uporabnik, namenski program, spletna kategorija),
51. konfiguriranje FW v polni funkcionalnosti, vpogled in analiziranje logov je dostopno lokalno na požarni pregradi, brez potrebe po dodatnih napravah, programski opremi ali licencah,
52. uporabniški vmesnik je grafičen (GUI), dostop in upravljanje preko tega vmesnika sta možna brez uporabe namenskih aplikacij, ampak s splošnimi klienti (HTTP/HTTPS – poljuben brskalnik),
53. omogoča grafično in objektno orientirano pisanje varnostnih pravil v prejšnji točki opisanemu grafičnem vmesniku (združevanje objektov v skupine, negiranje polj, uporaba več objektov kot vir ali cilj prometa znotraj enega pravila),
54. požarna pregrada zagotavlja preglednost ter zmožnost identifikacije in omejevanja aplikacij, ne glede na port, protokol, izmikajoče se tehnike ali šifriranje (TLS/SSL) ali uporabo nestandardnih portov, znotraj enega samega varnostnega pravila,
55. konfiguracija vseh funkcionalnosti je mogoča preko obeh vmesnikov: CLI in GUI,
56. požarna pregrada omogoča overjanje uporabnikov tudi preko oblačnih ponudnikov (identitiy provider - IdP) preko SAML 2.0 protokola,
57. požarna pregrada omogoča pridobivanje podatkov o uporabnikih tudi iz oblačnih ponudnikov (identitiy provider - IdP) za zagotavljanje ZTNA v vseh okoljih,
58. proizvajalec požarne pregrade zagotavlja konstanto spremljanje stanja požarne pregrade glede zasedenosti virov, kritičnih dogodkov ter skladnosti konfiguracije s priporočili dobre prakse (AIOps),
59. požarna pregrada podpira VPN za oddaljeni dostop (preko SSL, IPsec, brez odjemalca (ang.clientless)). Poleg tega omogoča preprečevanje mobilnih groženj (mobile threat prevention) in koristenje politik na podlagi aplikacij, uporabnikov, vsebine, naprave in stanja naprave,
60. požarna pregrada podpira avtomatski povratek (ang. fallback) na SSL VPN iz IPSec VPN,
61. požarna pregrada podpira VPN povezave iz naslednjih platform: Microsoft Windows in Apple macOS,
62. požarna pregrada podpira horizontalno skaliranje števila VPN uporabnikov v primeru, da je to potrebno, z uporabo dodatnih NGFW naprav v konfiguraciji brez visoke razpoložljivosti (tj. samostojno),
63. naprava omogoča dobro dokumentiran in varen programabilni spletni vmesnik (API) za upravljanje naprave preko API klicev z namenom integracije z naročnikovimi obstoječimi ali bodočimi sistemi za varnostno orkestracijo in samodejno kibernetsko obrambo,
64. naprava omogoča uporabo dinamičnih skupin objektov in urejanje članstva v dinamičnih skupinah brez ponovne instalacije (install/deploy/commit) politike naprave,
65. lokalni grafični uporabniški vmesnik (GUI) požarne pregrade in/ali opcijska zunanja centralna upravljalna platforma ponujata možnost pregleda razpoložljivih različic programske opreme ter možnost prenosa in aktivacije programskih verzij znotraj njunih vmesnikov,
66. lokalni GUI podpira neposreden prenos in aktivacijo programskih verzij brez odvisnosti od zunanjih orodij ali centralne upravljalne platforme,
67. lokalni grafični vmesnik (GUI) natančno odraža delujočo konfiguracijo požarne pregrade, ne glede na to, ali je bila prvotno posredovana s centralne upravljalne platforme ali konfigurirana lokalno,
68. požarna pregrada podpira označevanje in prekategorizacijo QoS na podlagi izvornega/ciljnega IP-ja, porta, protokola in aplikacije.

2.5. Zahtevani optični moduli in povezovalni kabli

Naročniku bomo dobavili šestnajst (16) kosov 10G SFP+ optičnih modulov kompatibilnih s ponujeno opremo ter osem (8) pripadajočih povezovalnih optičnih kablov dolžine 5 metrov. Navedeno se lahko nadomesti z osem (8) 10G SFP+ AOC pripravljenih povezovalnih kablov dolžine 5 metrov.

2.6. Zahtevana programska oprema, naročnine in licence:

- programska oprema zagotavlja vse zgoraj zahtevane funkcionalnosti,
- v primeru, da je za delovanje zgoraj naštetih funkcionalnosti potreba ustrezna licenca ali naročnina, je vključena za ves čas trajanja pogodbe;
- aktivacija/e, naročnina/e, licenčnina/e in vzdrževanje za vse zgoraj navedene zahteve/funkcionalnosti so zajete v ponudbeni ceni in naročniku ne bodo povzročili dodatnih stroškov.

3. Lokacija in obseg izvajanja storitev

Naročniku zagotavljamo dobavo opreme in izvedbo storitev na njegovih lokacijah v Ljubljani in Kopru. Na obeh lokacijah naročniku zagotavljamo izvedbo naslednjih storitev:

1. vzpostavitev HA para v telekomunikacijsko omarico, povezava v obstoječe omrežje, povezava HA in MGMT vmesnikov,
2. osnovna konfiguracija (HA, Management, licenciranje, posodobitev),
3. priprava izvedbenega načrta migracije,
4. čiščenje neuporabljenih objektov in pravil, varnostna optimizacija varnostnih pravil in pravil NAT,
5. izvoz obstoječe konfiguracije in uvoz na novo opremo,
6. priprava VPN infrastrukture, uvedba centraliziranega RAVPN dostopa, integracija z aktivnim imenikom,
7. implementacija multifaktorske avtentikacije za VPN dostop,
8. konfiguracija varnostnih pravil glede na identitete uporabnikov,
9. vključevanje naprednih NGFW funkcionalnosti na pravilih (DNS Security, AS, IPS,...),
10. selitev URL politike iz forward proxy na NGFW,
11. prestavitev BGP peering iz obstoječih usmerjevalnikov na NGFW,
12. optimizacija varnostnih pravil – izbris neuporabljenih pravil, združevanje pravil, migracija pravil.

4. Rok za dobavo in namestitev opreme

Naročniku zagotavljamo, da smo sposobni dobaviti, namestiti in konfigurirati opremo ter opraviti primopredajo obeh požarnih pregrad (vključno s tehnično dokumentacijo) in opraviti vse storitve, ki so predmet javnega naročila, v roku 90 dni od dneva podpisa pogodbe.

5. Garancijski pogoji

Garancija za vso dobavljeno komunikacijsko strojno opremo je 36 mesecev in je všteta v ceno.

Za pripadajočo programsko opremo veljajo garancijski in licenčni pogoji, kot jih proizvajalec te opreme nudi za posamezne programske proizvode.

Garancijski rok začne teči od dneva podpisa dobavnice. Če je bila oprema v garancijskem roku zamenjana ali bistveno popravljena, začne garancijski rok znova in je prodajalec dolžan izdati nov garancijski list.

Dobava in namestitev rezervnih delov ter vsi drugi stroški v zvezi s popravilom v času garancijskega roka bremenijo dobavitelja / izvajalca.

Dobavitelj / izvajalec ne jamči v naslednjih primerih:

- če naročnik z opremo ni ravnal po navodilih za uporabo, ki so priložena izdelkom,
- če je v izdelek posegla nepooblaščena oseba,
- če naročnik nestrokovno in malomarno ravna z izdelkom.

Garancija ne pokriva:

- okvar, povzročenih pri transportu po izročitvi blaga,
- mehanskih okvar, ki jih povzroči naročnik,

- okvar, povzročenih zaradi nihanja električne napetosti ali udarov strele in prenapetostnega udara,
- okvar, povzročenih zaradi neustrezne temperature ali vlage,
- okvar, povzročenih zaradi višje sile.

6. Režim garancijskega vzdrževanja opreme

V primeru sklenitve pogodbe bomo naročniku zagotovili možnost, da lahko prijavi napako 24 ur in 7 dni v tednu.

V primeru nepravilnega delovanja programske opreme bomo naročniku nudili tehnično pomoč in obvestili proizvajalčev center za tehnično pomoč o zaznani napaki.

Ko proizvajalec dobavi novo različico programske opreme, bomo v dogovoru z naročnikom namestiti novo programsko opremo.

V primeru prijave okvare do 12. ure bomo okvaro na opremi odpravili v istem delovnem dnevu, v primeru prijave okvare po 12. uri zagotavljamo odpravo napake na opremi najpozneje naslednji delovni dan.

Garancijsko vzdrževanje vključuje tudi:

1. vodenje vseh postopkov prijave, obravnave in odprave napak pri proizvajalcu,
2. neposreden (7x24x365) dostop do proizvajalčevega centra za tehnično pomoč,
3. dostop do novih verzij programske opreme,
4. pravico do vseh novih verzij programske opreme (v okviru funkcionalnosti), kot jih dobavlja proizvajalec opreme,
5. obveščanje naročnika o novih verzijah in spremembah v njih
6. vodenje dokumentacije vzdrževalnih posegov na opremi naročnika tako, da je naročniku zagotovljena možnost vpogleda v dokumentacijo preko interneta za čas trajanja pogodbe,
7. obveščanje naročnika o varnostnih problemih z obstoječimi verzijami programske opreme in takojšnja izvedba akcij v dogovoru z naročnikom, če obstaja varnostna ogroženost na opremi, ki jo ima naročnik;
8. dostop do tehnoloških informacij proizvajalca opreme v času trajanja te pogodbe.

Ob sklenitvi pogodbe bomo naročniku posredovali telefonsko številko in elektronski naslov, na katerem je dosegljiv nadzornik sistema.

Naročniku zagotavljamo, da se bo komunikacija s klicnim centrom in našim tehničnim osebjem izvajala v slovenskem jeziku.

Naročniku bomo omogočili, da lahko kadarkoli med izvajanjem pogodbe preveri nivo zagotavljanja storitve.

V _____ dne _____

_____

(osebno ime, funkcija in lastnoročni ali elektronski podpis)

Navodilo UJP:

V primeru skupne ponudbe obrazec izpolni in podpiše vodilni oziroma poslovodeči partner poslovne skupine ali konzorcija.

Uporaba žiga na dokumentu ni obvezna, če je dokument podpisan z varnim digitalnim podpisom, overjenim s kvalificiranim digitalnim potrdilom, ali če ponudnik v skladu z notranjimi akti žiga ne uporablja.

Ponudnik k temu obrazcu priloži tehnično dokumentacijo, v kateri predstavi konfiguracijo in tehnične lastnosti ponujene opreme (opisi, slike, grafikoni, prospekti, katalogi, specifikacije)

Tehnična dokumentacija proizvajalca opreme je lahko priložena v angleškem jeziku.

Obrazec 4 – Izjava o tehnični in strokovni sposobnosti

Ponudnik: _____

_____

_____

(ime in naslov)

IZJAVA O TEHNIČNI IN STROKOVNI SPOSOBNOSTI

Pod materialno in kazensko odgovornostjo izjavljamo, da smo sposobni zagotoviti kadrovsko in tehnično sposobnost za izvajanje storitev namestitve in konfiguracije ter garancijskega vzdrževanja ponujene opreme, oziroma, da izpolnjujemo naslednje zahteve in pogoje:

1. da imamo najmanj tri (3) certificirane strokovnjake, ki imajo certifikate z napredno ravnijo tehničnega znanja za ponujene rešitve s področja mrežne varnosti, kot na primer PCNSE za Palo Alto Networks ali enakovreden certifikat drugega proizvajalca, ki ga izda proizvajalec opreme,
2. da imamo pridobljen certifikat Cisco Preferred Security Partner (ali višji Cisco) ali enakovreden certifikat ali enakovreden status pri proizvajalcu / principalu druge ponujene enakovredne opreme;
3. da imamo za potrebe migracije najmanj dva (2) eksperta za izvajanje storitev namestitve in konfiguracije opreme za področje varnosti (kot na primer certifikat Cisco Certified Internetwork Expert - CCIE) oziroma ekvivalentni certifikat drugega proizvajalca enakovredne opreme);
4. da vsi naši strokovnjaki, ki bodo sodelovali pri izvedbi naročila, aktivno govorijo slovenski jezik (nivo B2 v skladu s CEFR);
5. da imamo veljavno poslovno povezavo s principalom – proizvajalcem ponujene opreme, ki nam omogoča dostop do tehnične podpore in zagotavlja podporo pri reševanju težav v delovanju in upravljanju požarnih pregrad.

V _____ dne _____

_____

(osebno ime, funkcija in lastnoročni ali elektronski podpis)

DOKAZILA:

- veljavni certifikati ali potrdila o strokovni usposobljenosti kadrov,
- dokazilo za aktivno znanje slovenskega jezika: spričevalo o izobrazbi, pridobljeni v Republiki Sloveniji, kjer je bil pouk v slovenščini (npr. matura, diploma, srednješolsko spričevalo), ali - potrdilo o opravljenem izpitu iz znanja slovenskega jezika na ustrezni ravni (B2), ki ga izdajo pooblaščene institucije, kot so: Center za slovenščino kot drugi/tuji jezik (Filozofska fakulteta UL) ali drugi javni izobraževalni zavodi, ki izvajajo preizkuse znanja jezika,
- certifikat ali pisna izjava proizvajalca strojne in programske opreme ali pooblaščenega principala, iz katere je razvidno, da ima ponudnik opreme status partnerja, ki mu omogoča dostop do tehnične podpore in zagotavlja podporo pri reševanju težav v delovanju in upravljanju požarnih pregrad.

Navodilo UJP:

- *V primeru skupne ponudbe obrazec izpolni in podpiše vodilni oziroma poslovodeči partner poslovne skupine ali konzorcija.*
- *Ponudnik se lahko sklicuje na kadrovske kapacitete (redno zaposlene delavce) in tehnično sposobnost drugih gospodarskih subjektov, ki bodo sodelovali pri izvedbi tega naročila, kot partnerji skupne ponudbe ali podizvajalci.*
- *Ponudnik k temu obrazcu priloži zgoraj navedena dokazila.*
- *Tehnične dokumentacije in certifikatov proizvajalca opreme, izdanih v angleškem jeziku, ni potrebno prevesti v slovenski jezik.*

Obrazec 5 – Referenčno potrdilo

Referenčni naročnik: _____

_____

_____

(ime in naslov)

Kontaktna oseba: _____

_____

_____

(ime in priimek, telefon, e-naslov)

Na prošnjo gospodarskega subjekta:

_____

(naziv in naslov gospodarskega subjekta)

pod kazensko in materialno odgovornostjo **izjavljamo**,

- da je navedeni gospodarski subjekt v obdobju od _____ do _____ po pogodbi št._____ /št. pogodbe/naročilnice/ z dne _____, sklenjeni z nami kot naročnikom, uspešno dobavil, namestil in konfiguriral najmanj dve (2) požarni pregradi v visoko razpoložljivostnem načinu delovanja;
- da je bila vrednost dobavljene opreme in izvedenih spremljajočih storitev najmanj 50.000,00 EUR brez DDV;
- da komunikacijsko omrežje, ki vključuje te naprave, uporablja najmanj 250 uporabnikov.

Potrjujemo, da so bile vse dobave opreme in storitve opravljene pravočasno, strokovno, kakovostno in v skladu z določili pogodbe/naročilnice, ter da proti izvajalcu nismo uveljavljali jamstev, kot so unovčenje bančnih garancij, kavcijskih zavarovanj zavarovalnic ali menic, plačila porokov, ter da do izvajalca nimamo odprtih sporov ali drugih zahtevkov, vezanih na navedeno pogodbo oziroma naročilnico.

Kraj:

Datum:

_____

(ime, priimek in naziv ali funkcija ter lastnoročni ali elektronski podpis odgovorne osebe potrjevalca reference)

Navodilo UJP:

Ponudnik se lahko sklicuje na reference podizvajalcev ali partnerjev skupne ponudbe.

Uporaba žiga na dokumentu ni potrebna, če je dokument podpisan z varnim digitalnim podpisom, overjenim s kvalificiranim digitalnim potrdilom, ali če referenčni naročnik v skladu z notranjimi akti žiga ne uporablja.

Obrazec 6 – Izjava tuje fizične osebe o nekaznovanosti

IZJAVA O NEKAZNOVANOSTI

Ime in priimek:	_____
Davčna številka ali druga identifikacijska številka v matični državi:	_____
Datum rojstva:	_____
Kraj rojstva:	_____
Država rojstva:	_____
Naslov stalnega/začasnega bivališča *(ulica in hišna številka, poštna številka in kraj)*:	_____
Državljanstvo:	_____

V zvezi s ponudbo, oddano v postopku javnega naročila *»Dobava, namestitev, konfiguracija in garancijsko vzdrževanje požarnih pregrad v komunikacijskem omrežju«,* z oznako 4/2026-JNMV-PP,

pod kazensko in materialno odgovornostjo **izjavljam**:

1. da mi ni bila izrečena pravnomočna sodba za kazniva dejanja iz Kazenskega zakonika (Uradni list RS, št. 50/12 - uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17, 23/20, 91/20, 95/21, 186/21, 105/22 – ZZNŠPP, 16/23, 107/24 – odl. US in 1564/26; v nadaljnjem besedilu: KZ-1) ali za primerljiva kazniva dejanja, ki so jih izrekla pristojna sodišča, ki so taksativno našteta v prvem odstavku 75. člena Zakona o javnem naročanju (Uradni list RS, št. 91/15, 14/18, 121/21, 10/22, 74/22 – odl. US, 100/22 – ZNUZSZS, 28/23, 88/23 – ZOPNN-F in 83/25 - ZOUL; v nadaljnjem besedilu: ZJN-3):

   - terorizem (108. člen KZ-1),
   - financiranje terorizma (109. člen KZ-1),
   - ščuvanje in javno poveličevanje terorističnih dejanj (110. člen KZ-1),
   - novačenje in usposabljanje za terorizem (111. člen KZ-1),
   - spravljanje v suženjsko razmerje (112. člen KZ-1),
   - trgovina z ljudmi (113. člen KZ-1),
   - sprejemanje podkupnine pri volitvah (157. člen KZ-1),
   - kršitev temeljnih pravic delavcev (196. člen KZ-1),
   - goljufija (211. člen KZ-1),
   - protipravno omejevanje konkurence (225. člen KZ-1),
   - povzročitev stečaja z goljufijo ali nevestnim poslovanjem (226. člen KZ-1),
   - oškodovanje upnikov (227. člen KZ-1),
   - poslovna goljufija (228. člen KZ-1),
   - goljufija na škodo Evropske unije (229. člen KZ-1),
   - preslepitev pri pridobitvi in uporabi posojila ali ugodnosti (230. člen KZ-1),
   - preslepitev pri poslovanju z vrednostnimi papirji (231. člen KZ-1),
   - preslepitev kupcev (232. člen KZ-1),
   - neupravičena uporaba tuje oznake ali modela (233. člen KZ-1),
   - neupravičena uporaba tujega izuma ali topografije (234. člen KZ-1),
   - ponareditev ali uničenje poslovnih listin (235. člen KZ-1),

- izdaja in neupravičena pridobitev poslovne skrivnosti (236. člen KZ-1),
- zloraba informacijskega sistema (237. člen KZ-1),
- zloraba notranje informacije (238. člen KZ-1),
- zloraba trga finančnih instrumentov (239. člen KZ-1),
- zloraba položaja ali zaupanja pri gospodarski dejavnosti (240. člen KZ-1),
- nedovoljeno sprejemanje daril (241. člen KZ-1),
- nedovoljeno dajanje daril (242. člen KZ-1),
- ponarejanje denarja (243. člen KZ-1),
- ponarejanje in uporaba ponarejenih vrednotnic ali vrednostnih papirjev (244. člen KZ-1),
- pranje denarja (245. člen KZ-1),
- zloraba negotovinskega plačilnega sredstva (246. člen KZ-1),
- uporaba ponarejenega negotovinskega plačilnega sredstva (247. člen KZ-1),
- izdelava, pridobitev in odtujitev pripomočkov za ponarejanje (248. člen KZ-1),
- davčna zatajitev (249. člen KZ-1),
- tihotapstvo (250. člen KZ-1),
- zloraba uradnega položaja ali uradnih pravic (257. člen KZ-1),
- oškodovanje javnih sredstev (257.a člen KZ-1),
- izdaja tajnih podatkov (260. člen KZ-1),
- jemanje podkupnine (261. člen KZ-1),
- dajanje podkupnine (262. člen KZ-1),
- sprejemanje koristi za nezakonito posredovanje (263. člen KZ-1),
- dajanje daril za nezakonito posredovanje (264. člen KZ-1),
- hudodelsko združevanje (294. člen KZ-1).

2. da država, v kateri imam prijavljeno stalno ali začasno prebivališče, potrdil iz kazenske evidence ne izdaja ali potrdila ne zajemajo vseh zgoraj navedenih kaznivih dejanj oziroma primerov iz prvega odstavka 75. člena ZJN-3;

3. da predmetna izjava, dana pred pristojnim sodnim ali upravnim organom ali notarjem v matični državi, velja kot dokazilo o neobstoju izključitvenega razloga iz prvega odstavka 75. člena v povezavi s četrtim odstavkom 77. člena ZJN-3.

Datum: _____

Kraj: _____

Podpisnik izjave: _____

(osebno ime in podpis

Potrdilo / žig in podpis pristojnega sodnega ali upravnega organa ali notarja

**Opomba naročnika / UJP: Ta obrazec / izjava velja izključno za fizične osebe, ki nimajo stalnega ali začasnega prebivališča na območju Republike Slovenije ter slovenske enotne matične številke občana (EMŠO), če so izpolnjeni pogoji iz 2. in 3. točke te izjave*