

**PROJEKTNI ZADATAK**

21UUINTR\_PRZ\_20210830

**PROJEKT**

 20UUINTR – Internet pristup za centralnu lokaciju MP

**POSLOVNI KORISNIK**

GLAVNO TAJNIŠTVO

**Nositelj PROJEKTA**

GLAVNO TAJNIŠTVO

SEKTOR ZA INFORMACIJSKE SUSTAVE I UPRAVLJANJE IMOVINOM

Sadržaj

[1. UVOD 2](#_Toc44497930)

[2. POSLOVNA POTREBA 2](#_Toc44497931)

[3. OPSEG ZADATAKA 2](#_Toc44497932)

[3.1. Pristup internetu 3](#_Toc44497933)

[3.2. Renundancija usluge pristupa internetu (sekundarni link) 3](#_Toc44497934)

[3.3. Sigurnosna zaštita od DDoS napada 3](#_Toc44497935)

[3.4. Tehnička podrška 6](#_Toc44497936)

[4. ZAHTJEVI ZA IZMJENAMA PROJEKTA 7](#_Toc44497937)

[5. NAČIN IZVRŠENJA AKTIVNOSTI 7](#_Toc44497938)

[6. UPRAVLJANJE PROJEKTOM 8](#_Toc44497939)

[7. FORMALNO ZATVARANJE PROJEKTA 8](#_Toc44497940)

[8. VERIFIKACIJA I PLAĆANJE 8](#_Toc44497941)

[9. POSLOVNA TAJNA 9](#_Toc44497942)

## UVOD

Pristup internetu je mogućnost pojedinaca i organizacija za povezivanje s internetom putem računalnih terminala, računala i drugih uređaja, i za pristup uslugama kao što su e-pošta i svjetska mreža. Ministarstvo poljoprivrede ima potrebu za uslugom pristupa internetu, a koja je namijenjena poslovnim korisnicima s povećanim zahtjevima.

## POSLOVNA POTREBA

Potrebno je osigurati sigurnosni i neometani pristup internetu za centralnu lokaciju Ministarstva poljoprivrede s neograničenim prometom, na način da je primarni pristup internetu kapaciteta 200 megabita po sekundi za preuzimanja i prijenos podataka.

Za pristup internetu mora se realizirati backup primarne usluge s istim obilježjima (kapaciteta 200 megabita po sekundi za preuzimanja i prijenos podataka). Trase primarnog i sekundarnog linka moraju biti fizički odvojene te se nigdje ne smiju preklapati.

Potrebno je osigurati pristup internetu sa sigurnosnom zaštitom od potencijalnih DDOS napada dediciranim DDoS sustavom smještenim unutar mreže pružatelja usluge.

Potrebno je osigurati tehničku podršku u slučaju problema s isporukom usluge i prekidom poslovanja Naručitelja uslijed nedostupnosti usluge.

## OPSEG ZADATAKA

Ponuditelj mora osigurati Naručitelju isporuku usluge tijekom 12 mjeseci.

Usluga se dijeli na podusluge:

* Pristup internetu
* Redundancija usluge pristupa internetu (sekundarni link)
* Sigurnosna zaštita od DDoS napada
* Tehnička podrška

Svaka podusluga detaljno je obrazložena u nastavku dokumenta.

Ponuditelj svojom uslugom mora zadovoljiti sljedeće uvjete:

* uključenje usluga najkasnije unutar 30 dana od sklapanja ugovora.
* ponuđeno rješenje ne smije iziskivati dodatna kapitalna ulaganja Naručitelja
* omogućiti Naručitelju uvid, nadzor, kontrolu i planiranje troškova usluga
* ponuđeno rješenje mora osigurati maksimalnu sigurnost mreže, uključivo zaštitu informacijsko – komunikacijskog sustava Naručitelja od pristupa trećih osoba s Interneta i iz drugih podatkovnih (korisničkih) mreža realiziranih na platformi Ponuditelja usluge,
* ponuditelj mora osigurati neprekinutost poslovanja Naručitelja

Ponuditelj mora jamčiti vrijeme pružanja usluga i tehničke podrške 24 sata na dan tijekom svih dana u godini. Točka razgraničenja odgovornosti za kvalitetu isporučene usluge između Naručitelja i Ponuditelja je sučelje na Ponuditeljevoj opremi (CPE-oprema na strani korisnika) na koje se spaja oprema u nadležnosti Naručitelja.

Ponuditelj i Naručitelj obvezuju se međusobno razmijeniti informaciju o autoriziranim osobama, njihovim fiksnim i mobilnim brojevima telefon, kao i o e-mail adresama. Ponuditelj je dužan za Naručitelja osigurate kompetentne osobe po pitanju logističke podrške za Naručitelja, KAM-a (Key Account Manager), a po pitanju tehničke podrške TAM-a (Technical Account Manager) za sve vrijeme trajanja ugovora.

### Pristup internetu

Potrebno je osigurati sigurnosni i neometani pristup internetu za centralnu lokaciju Ministarstva poljoprivrede s neograničenim prometom, na način da je primarni pristup internetu kapaciteta 200 megabita po sekundi za preuzimanja i prijenos podataka. Ponuditelj je obvezan realizirati stalnu vezu na Internet uz pomoć svjetlovodnih kabela, u roku od maksimalno 30 dana od dana sklapanja ugovora, bez prekida Internet prometa Naručitelja.

Ponuditelj mora osigurati pouzdanost i raspoloživost Internet pristupa, te garantiranu brzinu pristupa do Internet okosnice. Ponuditelj mora dokazati da je spojen na globalnu Internet mrežu putem minimalno dva (2) nezavisna up-stream davatelja usluga i to fizičkim vodovima.

Naručitelj u svakom trenutku, uz prethodnu obavijest Ponuditelju, ima pravo priključiti i aktivirati na krajnjem uređaju primarnog linka Ponuditelja senzor/e alata za nadzor infrastrukture (Zabbix, PRTG, UIM ili slično) kako bi imao ažuriran prikaz stanja, raspoloživosti i uvjeta (prometa) usluge.

### Renundancija usluge pristupa internetu (sekundarni link)

Pouzdanost i raspoloživost pristupa internetu kao osnova za neprekinutost poslovanja Naručitelja mora se realizirati kroz uspostavu backupa primarne usluge s istim obilježjima (brzina backup-a ista je brzini primarne usluge). Trase primarnog i sekundarnog (backup) linka moraju biti fizički odvojene i nigdje se ne smiju preklapati. Sekundarni link podrazumijeva redundantnu terminalnu opremu na krajnjim lokacijama i odgovarajuću redundanciju u samoj mreži Ponuditelja, kako na prihvatnom dijelu tako i u čitavom koru.

Naručitelj u svakom trenutku, uz prethodnu obavijest Ponuditelju, ima pravo priključiti i aktivirati na krajnjem uređaju sekundarnog linka Ponuditelja senzor/e alata za nadzor infrastrukture (Zabbix, PRTG, UIM ili slično) kako bi imao ažuriran prikaz stanja, raspoloživosti i uvjeta (prometa) usluge.

### Sigurnosna zaštita od DDoS napada

Kako bi sigurnosna zaštita pristupa internetu od potencijalnih ugroza bila uspostavljena, Ponuditelj je dužan osigurati naprednu zaštitu internet resursa Naručitelja na stalnim vezama.

Pristup Internetu mora biti zaštićen od potencijalnih DDoS napada dediciranim DDoS sustavom renomiranog svjetskog proizvođača. Sustav mora prikupljati i analizirati promet, proaktivno detektirati DDoS napade, te vršiti „čišćenje“ (mitigaciju) malicioznog prometa kako ne bi došlo do značajnijeg pada u kvaliteti na brojnim servisima koji koriste predmetnu vezu.

Promet koji se analizira i štiti je sav promet koji dolazi s internet mreže, neovisno o upstream davatelju internet usluga, ali i promet koji dolazi od korisnika lokalnog pružatelja usluge pristupa Internetu. Cijeli sustav mora biti lociran unutar mreže pružatelja usluge pristupa Internetu, čime je osigurano da se korisnički promet ni u jednom trenutku ne prosljeđuje trećim stranama za potrebe njegovog „čišćenja“.

Traži se sustav DDoS zaštite svjetski renomiranog proizvođača koji omogućuje minimalno sljedeće:

* stalni nadzor mrežnog prometa putem web sučelja
* zaštitu od volumetričnih DDoS napada
* zaštitu od različitih tipova aplikacijskih napada (HTTP, DNS, VoIP…)
* real-time sustav obavještavanja i izvještavanja (alerting&reporting)
* mogućnost forenzičke analize napada i izradu izvještaja

**DDoS sustav mora sadržavati sljedeće komponente**

**A STATISTIKA DDoS NAPADA**

**B Komponente ADDoS platforme**

**B.1 kolektor**

1. Skupljanje netflow/SNMP paketa s rutera

2. Skupljanje routing tablica (bgp) s nadziranih rutera

3. Analiza mrežnog prometa

4. Detekcija prometnih anomalija i napada

5. Alarmiranje

6. Reporting

**B.2 mitigacija**

 Oglašavanje rute za preusmjeravanje prometa na TMS

 Prihvat legitimnog i zlonamjernog prometa

 Analiza preusmjerenog prometa (L7)

o detekcija tipa napada

o Zadavanje mjera za čišćenje prometa

o Isporučivanje očišćenog prometa prema žrtvi

**B.3 Portal Interface**

• WEB pristup (HTTPS)

• GUI funkcionalnost kao na SP-u

• Instalirano na virtualnoj mašini

• Rasterećenje SP

**C. Izvještaji**

 Mogućnost kreiranja više tipova izvještaja s različitim podacima:

o Promet po određenim aplikacijama,

o Lista alarma,

o Broj mitigacija po tipu

o Broj mitigacija po trajanju

 Slanje periodičnih izvještaja (mjesečni)

 Slanje izvještaja na mail adresu

Ponuditelj u sklopu ponuđenog DDoS sustava/usluge mora osigurati mogućnost nadogradnje/proširenja korištenja sustava na način da se omogući izravan uvid u mrežni promet te detekcija i zaštita od DDoS napada u stvarnom vremenu u svrhu brže reakcije i pokretanja (automatskog i ručnog) procesa mitigacije u slučaju volumetric napada.

Ponuda DDoS sustava mora uključivati:

• opis rješenja

• lokaciju gdje se sustav nalazi

• vremena odziva u slučaju napada

Također, Ponuditelj je dužan po potrebi pružiti i podršku „tradicionalnim“ metodama filtriranja prometa pristupnim listama na rubnim usmjerivačima ponuditeljima.

Ponuditelj za zaštitu od DDoS napada mora osigurati alternativni pristup portalu preko kojeg korisnik ima uvid o prometu, alarmima, mitigacijama i sl.

Pristup portalu treba biti omogućen i putem USB mobilnog sticka (ili sličnim alternativnim rješenjem) gdje Ponuditelj ovime omogućuje krajnjem korisniku siguran pristup portalu putem dediciranog APNa u slučaju da je pod DDoS napadom i da zbog napada ne može pristupiti portalu iz svoje mreže

### Tehnička podrška

Ponuditelj mora jamčiti vrijeme pružanja usluga i tehničke podrške 24 sata na dan tijekom svih dana u godini.

Točka razgraničenja odgovornosti za kvalitetu isporučene usluge između Naručitelja i Ponuditelja je sučelje na Ponuditeljevoj opremi (CPE-oprema na strani korisnika) na koje se spaja oprema u nadležnosti Naručitelja.

Ponuditelj se obvezuje svaku prijavu kvara/smetnje, od strane Naručitelja, zaprimiti telefonskim putem na broj za prijavu i/ili elektroničkom porukom na prijavnu adresu.

Prijava treba sadržavati osnovne podatke o smetnji, vrijeme nastanka, način registracije, utjecaj na sustav i usluge, poduzetim koracima do tog trenutka i ostale korisne informacije. Prioritet pogreške utvrđuju se zajednički. Potvrda o zaprimljenoj prijavi kvara/smetnje nakon provjere od strane Ponuditelja bit će poslana elektroničkom porukom Naručitelju.

Tehnička podrška podrazumijeva podršku na mrežnoj opremi Ponuditelja.

Tražimo tehnički dediciranu osobu (Single Point Of Contact) od strane Ponuditelja koja će biti zadužena za podršku i brže rješavanje problema za uslugama koje ponuditelj nudi. Usluga mora sadržavati sljedeće komponente vezane za podatkovne i sve usluge tražene natječajem s posebnim naglaskom na područja iz:

•           IT Mreže

•           Sigurnost

Obzirom da Naručitelj na svojoj mreži koristi isključivo mrežnu Cisco opremu te na kompleksnost poslovanja, visoku dostupnost usluga i osjetljivost podataka koja je neophodna za uredno poslovanje, tražimo da Ponuditelj svoje tehničke kompetencije dokazuje sa minimalno 2 certficirana Cisco CCIE (Routing & Switching) stručnjaka ili jednakovrijednim certifikatom.

Ponuditelj je dužan dostaviti ime prezime,  broj mobitela, mail te stručnu spremu dedicirane osobe koja će biti dodijeljena za tehničku podršku.

Također je dužan dostaviti ime prezime, broj telefona i mail stručnjaka sa Cisco CCIE (Routing & Switching) certifikatima koje Naručitelj može kontaktirati po potrebi,.

Zaprimljene prijave podliježu sljedećim rokovima za rješavanje:

|  |  |  |
| --- | --- | --- |
| **Prioriteti prema hitnosti** | **Vrijeme odziva** | **Vrijeme pronalaženja i otklona smetnje** |
| Stupanj ozbiljnosti 1: Kritičan Potpuni prekid rada usluge na lokaciji Naručitelja | < 15 minuta | < 4 sata |
| Stupanj ozbiljnosti 2: Ozbiljan Pogreške u radu usluge, narušena kvaliteta rada usluge i otežan rad na lokaciji Naručitelja | < 15 minuta | < 8 sati |
| Stupanj ozbiljnosti 3: UpozoravajućiSmetnja koja direktno ne utječe na korištenje usluge ili vrlo malo na lokaciji Naručitelja | 1 radni dan | 24 sata |

Vrijeme odziva definira se kao maksimalno vrijeme od trenutka prijavljivanja kvara/smetnje do trenutka potvrde Ponuditelja. Vrijeme povratne informacije prema Naručitelju za potpuni prekid usluge je maksimalno 15 minuta od prijave smetnje, a može biti putem telefona, elektroničke poruke ili nekog drugog dogovorenog načina komunikacije.

Vrijeme pronalaženja i otklona kvara/smetnje je vrijeme tokom radnog vremena Naručitelja između odziva i vremena otklanjanja smetnje, odnosno vraćanja u ispravno stanje. Naručitelj može u svako doba zatražiti podrobne podatke o statusu smetnje putem pozivanja Ponuditeljevog centra za korisnike ili TAM-a.

Ponuditelj je suglasan da snosi sve troškove intervencije (troškove dolaska i rada) prouzročene svojom greškom.

## ZAHTJEVI ZA IZMJENAMA PROJEKTA

Ukoliko se, tijekom izvođenja projekta, ukaže potreba za promjenom opsega poslova ili usluga, ista će se primijeniti samo u slučaju odobrenja promjene od strane Naručitelja (MP) i usuglašena s Ponuditeljem uz uvjet nemijenjanja vrijednosti financijskog iznosa ugovora.

Svaka promjena koja će biti zahtijevana od strane Naručitelja mora biti provedena u skladu sa službenom procedurom za upravljanje projektima Ministarstva poljoprivrede.

## NAČIN IZVRŠENJA AKTIVNOSTI

Ponuditelj će obavljati sve tražene aktivnosti sukladno zakonu struke i u skladu s normama ISO 27001 i ISO 9001.

Ponuditelj se obvezuje osigurati stručne, materijalne i sve druge (potrebne) preduvjete za izvršenje aktivnosti.

Ponuditelj će obveze preuzete ovim projektnim zadatkom obavljati po pravilima struke, vodeći se najvišim profesionalnim, etičkim i stručnim standardima. Ponuditelj odgovara za kvalitetno, profesionalno i pravovremeno obavljen posao naveden u opsegu poslova.

Ako se izvršenje aktivnosti odvija na lokaciji Naručitelja, djelatnici Ponuditelja će o svom dolasku u prostorije Naručitelja, o učinjenom poslu i o odlasku obavijestiti ovlaštene predstavnike - djelatnike Naručitelja.

## UPRAVLJANJE PROJEKTOM

Ponuditelj se obavezuje sve projektne aktivnosti provoditi u skladu s procedurom upravljanja projektima Ministarstva poljoprivrede. Naručitelj će dostaviti Ponuditelju dokumentaciju procedure upravljanja projekata te definirati djelatnike koji će ispred Ministarstva poljoprivrede upravljati projektom. Delegirana osoba predstavlja osnovni kanal komunikacije Naručitelja prema voditelju projekta Ponuditelja i u svoj komunikaciji obavezno mora biti uključena.

Naručitelj zadržava pravo prihvatiti ili odbiti prijedloge Ponuditelja za dopunama obrazaca dokumentacije procedure upravljanja projektima Ministarstva poljoprivrede s ciljem poboljšanja i pojednostavljenja procesa, sadržaja ili nužnih dokumenata.

## FORMALNO ZATVARANJE PROJEKTA

Isporukom i potpisivanjem projektne dokumentacije Ponuditelj ostvaruje uvjete za formalno zatvaranje projekta i potpisivanje Izjave o zatvaranju projekta te dobivanje potvrde Naručitelja o uredno izvršenoj usluzi koju može koristiti u budućim procesima javne nabave.

Ukoliko se u potpunosti ne realizira dostava dokumentacije te Ponuditelj ne ostvari uvjete za formalno zatvaranje projekta, Ministarstvo poljoprivrede nema nikakvu obvezu davati Ponuditelju potvrdu o uredno izvršenoj usluzi, a ujedno Ministarstvo poljoprivrede može kreirati internu „crnu listu“ u kojoj će voditi evidencije o neurednim izvršiteljima usluge te iste može uzimati u obzir i negativno bodovati prilikom kreiranja kriterija budućih javnih nabava.

## VERIFIKACIJA I PLAĆANJE

Plaćanje se vrši po izvršenju usluge. Procedura verifikacije izvršenja usluge:

* isporuka stavke troškovnika (mjesečni račun za uslugu)
* formalizirana dokumentom YYSFPROJ\_EPI\_YYYYMMDD (Evidencija projektnih isporučevina)
* Ponuditelj stječe uvjete za pripremu i isporuku Naručitelju računa za tu stavku
* dokumenti se Naručitelju dostavljaju elektroničkim putem (usluga E-Račun)
* e-računu obavezno se prilaže YYSFPROJ\_EPI\_YYYYMMDD (Evidencija projektnih isporučevina)
* zaprimanjem računa, provjera priložene dokumentacije, ukoliko je ispravna, verificira se
* Naručitelj ima obvezu plaćanja u roku 30 dana od zaprimanja računa u svoj elektronički sustav za obradu računa.

## POSLOVNA TAJNA

Ponuditelj se obvezuje da će podatke tehničkog i poslovnog značaja do kojih ima pristup pri izvršavanju ovog projektnog zadatka čuvati kao poslovnu tajnu. U slučaju da je jedna od strana u projektu odredila za neke podatke viši stupanj tajnosti – primjenjivati će se zakonske odredbe predviđene za određeni stupanj tajnosti.

Obveza čuvanja tajne ostaje i nakon ispunjenja ovog projektnog zadatka, sukladno najvišim propisanim standardima, a u roku od dvije godine od dana isteka ovog projektnog zadatka. Ovaj projektni zadatak ne priječi strane u projektu da se dalje dodatno obvezuju u pogledu zaštite poslovne tajne. U slučaju sukoba između odredbi tih nadopuna i prvotnih odredbi ovog projektnog zadatka, primjenjivati će se odredbe tih nadopuna.

U slučaju izravnog ili neizravnog otkrivanja podataka tehničkog i poslovnog značaja od strane Ponuditelja projekta, Ponuditelj se obvezuje naknaditi Naručitelju svaku štetu koju Naručitelj može trpjeti kao rezultat neovlaštene uporabe ili otkrivanja spomenutih podataka ovog projektnog zadatka od strane Ponuditelja.