Nabava softverski definiranog mrežnog pristupnog sustava sa sigurnosnom komponentom (Secure SDWAN)

Obavijest gospodarskim subjektima s ciljem prethodnog istraživanja tržišta

Sadržaj

1. Uvod

1.1. Općenito o projektu e-Sveučilišta

Sukladno Odluci ministra znanosti i obrazovanja od 22. veljače 2022. o utvrđivanju unaprijed određenog prijavitelja za provedbu aktivnosti predviđenih kroz investiciju C.3.1.R2-I1, „Digitalna preobrazba visokog obrazovanja“, Nacionalnog programa oporavka i otpornosti 2021.-2026., Hrvatskoj akademskoj i istraživačkoj mreži - CARNET, dodijeljena je nadležnost nositelja projekta „e-Sveučilišta“. Cilj projekta „e-Sveučilišta“ je omogućiti fleksibilizaciju obrazovanja kroz podršku učinkovitoj digitalnoj preobrazbi i povećanju digitalne zrelosti visokog obrazovanja, fokusiranu na krajnje korisnike, javno obrazovne ustanove u visokom obrazovanju. Predmetnom investicijom planirana su ulaganja u digitalnu nastavnu infrastrukturu i servise, opremu, alate i sadržaje, aktivnosti kibernetičke sigurnosti, unaprjeđenje postojećeg informatičkog sustava i evidencija u visokom obrazovanju te osnaživanje kompetencija nastavnog osoblja za učenje i poučavanje u digitalnom okruženju. Projekt „e-Sveučilišta“ započeo je s provedbom 23. ožujka 2022. dok se završetak svih aktivnosti planira realizirati do kraja 2025. godine.

CARNET provodi projekt e-Sveučilišta s ciljem digitalne preobrazbe visokog obrazovanja (VO) u Republici Hrvatskoj (RH) poboljšanjem digitalne nastavne infrastrukture, uvođenjem digitalnih nastavnih alata te osnaživanjem digitalnih kompetencija nastavnika za poučavanje u digitalnom okruženju.

Ulaganjima u mrežnu i računalnu infrastrukturu, opremu za izradu i produkciju audio/video sadržaja te povezane servise (aplikacije, licence i alate podrške) te aktivnosti kibernetičke sigurnosti, osigurat će se ključni preduvjeti za nastavak digitalne preobrazbe ustanova visokog obrazovanja na području cijele RH.

1.2. Općenito o nabavi

Hrvatska akademska i istraživačka mreža – CARNET planira započeti postupak javne nabave softverski definiranog mrežnog pristupnog sustava sa sigurnosnom komponentom u sklopu projekta e-Sveučilišta.

Krajnji korisnici ovog projekta su javne ustanove visokog obrazovanja: javna visoka učilišta, sveučilišta i sastavnice, veleučilišta, fakulteti, visoke škole i kampusi.

Cilj ove nabave je nadogradnja pristupne mrežne infrastrukture lokacija ustanova uključenih u projekt, čime će ustanove dobiti napredno upravljanje mrežnim i sigurnosnim funkcijama uz osiguranu kvalitetu, stabilnost i propusnost mrežne povezanosti na privatnu mrežu CARNET.

Sukladno Zakonu o javnoj nabavi (NN 120/16) sa svrhom pripreme nabave i informiranja gospodarskih subjekata o svojim planovima i zahtjevima u vezi s nabavom, u nastavku obavijesti CARNET objavljuje zahtjeve vezane za nabavu i isporuku softverski definiranog mrežnog pristupnog sustava sa sigurnosnom komponentom.

Radi daljnjeg planiranja i provedbe postupka nabave te izrade Dokumentacije o nabavi molimo sve zainteresirane gospodarske subjekte da dostave primjedbe i prijedloge prema traženim informacijama i troškovnikom najkasnije do 12.06.2023. na adresu elektroničke pošte nabava@carnet.hr.

CARNET će analizirati dostavljene informacije i temeljem dobivenih podataka sastaviti dokumentaciju o nabavi.

Prilikom provođenja istraživanja tržišta CARNET će postupati na način da svojim postupcima ne narušava tržišno natjecanje niti krši načela zabrane diskriminacije i transparentnosti.

Rezultati provedenog istraživanja ne obvezuju CARNET niti se stvara bilo kakav pravni posao ili odnos s gospodarskim subjektima koji sudjeluju u istraživanju.

2. Predmet nabave

Predmet ove nabave je softverski definirani mrežni pristupni sustav sa sigurnosnom komponentom (u nastavku Sustav) za javne ustanove visokog obrazovanja u Republici Hrvatskoj.

Predmet nabave podijeljen je na sljedeće cjeline:

1. Nabava sigurnosnih mrežnih (SD-WAN) uređaja TIP 1, 2, 3, 4. Nabavljeni sigurnosni mrežni uređaji implementirat će se na 218 lokacija ustanova (*endpoint* uređaji), 24 lokacije CARNET-ovih mrežnih čvorišta (*hub* uređaji) i dvije lokacije CARNET-ovih podatkovnih centara (*hub* uređaji). Tipovi uređaja se razlikuju prema podržanoj mrežnoj propusnosti uređaja, a sukladno očekivanim potrebama pojedinih lokacija korisnika. Na pojedine fizičke lokacije uslijed dvojake funkcije (CARNET čvorište i lokalna infrastruktura CARNET ustanove) biti će implementirano više posebnih sigurnosnih mrežnih uređaja. Na lokacijama ustanova sa najvećim opterećenjem bit će implementirana dva uređaja redundantno, a u podatkovnim centrima više neovisnih hub uređaja.
2. Nabava centraliziranog sustava za orkestraciju, upravljanje i nadzor sigurnosne SD-WAN mreže te integracija putem API poziva s postojećim sustavima Naručitelja. Sustav za orkestraciju, upravljanje i nadzor sigurnosne SD-WAN mreže mora podržati rad s novo implementiranim pristupnim mrežnim rješenjem putem web sučelja djelatnicima CARNET-a te svim imenovanim mrežnim administratorima ustanova koje sudjeluju u projektu.
3. Nabava usluge instalacije i konfiguracije mrežnog sustava, integracija s postojećom mrežom na lokaciji ustanove prema zahtjevima Naručitelja i predstavnika Ustanove i pripadajuća dokumentacija.
4. Nabava usluge edukacije korisnika u svrhu osposobljavanja za rad s novo isporučenim sustavom te pripadajući edukacijski materijali.
5. Nabavu naljepnica koje uključuju oznake vidljivosti (dalje u tekstu: naljepnice) i lijepljenje naljepnica na nabavljenu opremu.

Odabrani Ponuditelj jamči ispravan rad isporučene opreme i sustava navedenih pod točkama 1 i 2 tijekom jamstvenog roka. Trajanje i obveze tijekom jamstvenog roka određene su odredbama ove Dokumentacije i člancima 423.-428. primjenjivog Zakona o obveznim odnosima (NN 35/05, 41/08, 125/11, 78/15, 28/18).

Implementacija projekta uključuje isporuku i uspostavu cjelovite funkcionalnosti koja uključuje aktivnu mrežnu infrastrukturu te povezivanje opreme na centralni sustav Naručitelja. U sklopu projekta sustav će se implementirati na lokacijama definiranim u Prilogu 3. – Popis lokacija ustanova ove Dokumentacije.

Implementaciju opisanog u predmetu nabave potrebno je isporučiti kao cjelovit projekt kroz uspostavu cjelokupne funkcionalnosti aktivne mrežne infrastrukture te povezivanje sa središnjom mrežom Naručitelja, a sve prema zahtjevima Naručitelja opisanim u

nastavku dokumenta. Sve aktivnosti obuhvaćene predmetom nabave potrebno je izvršiti pridržavajući se pozitivnih propisa.

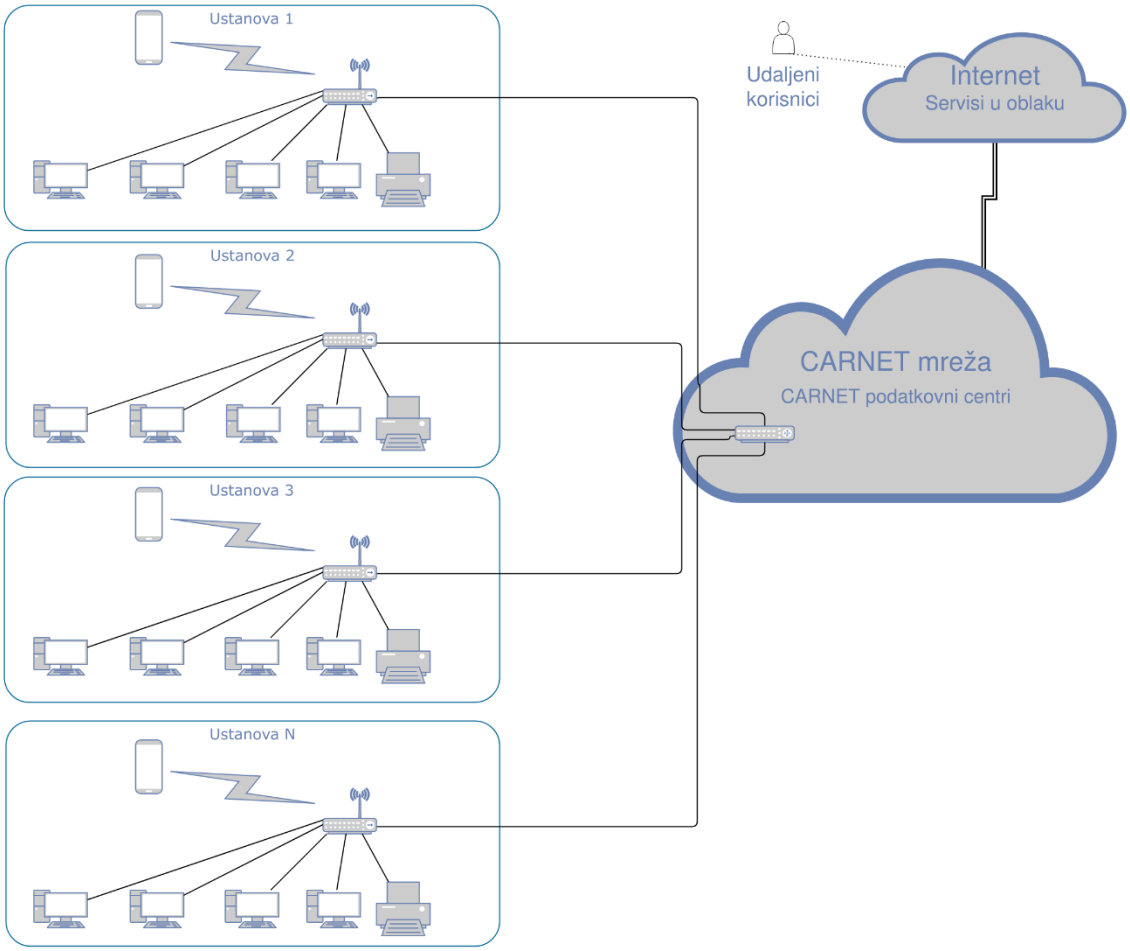
Sustav mora omogućiti:

- kibernetičku zaštitu ustanova - Unified Threat Management koji uključuje Statefull Firewall, Layer 7 Next Generation Firewall i Application Visibility, IPS/IDS, SSL inspekciju, web filtering, antivirus i antimalware;
- unaprjeđenje korisničkog iskustva mrežne povezivosti ustanova kroz proširenje dostupnih funkcionalnosti - virtualizacija i segmentacija pristupne mreže, centralizirano upravljanje politikama, orkestracija promjena i dinamičko upravljanje prometom;
- davanje ovlasti mrežnim administratorima na ustanovama za upravljanje i nadzor;
- naprednu analitiku i izvještavanje.

Sustav mora biti hardversko-softverski od istog proizvođača (single vendor) kako bi se osigurala interoperabilnost i zamijeniti će postojeću CARNET pristupnu opremu (CPE opremu – Customer Premises Equipment) na lokacijama ustanova. Odabrani Ponuditelj je dužan osigurati sav potreban hardware, software, licence i prespojne kabele potrebne za ispravno funkcioniranje cjelokupnog sustava.

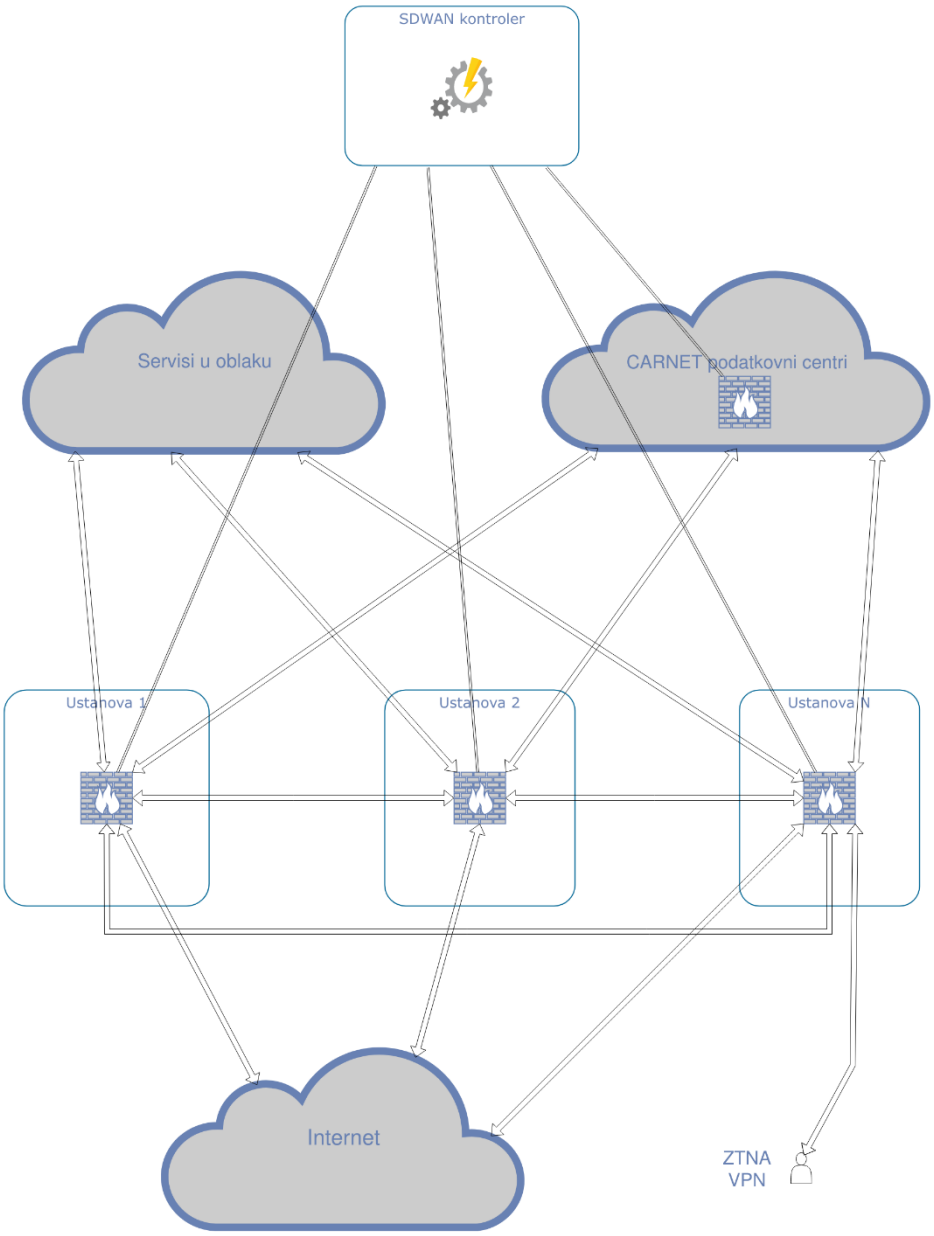
Troškovnikom definiranim u Prilogu 2. ove Dokumentacije, u sklopu nabave definirane su okvirne količine opreme za sve ustanove, a točni podaci količina po pojedinoj lokaciji ustanova bit će dostavljeni odabranom Ponuditelju nakon potpisa Ugovora o javnoj nabavi, a sukladno dinamici izvođenja.

Slika 1. prikazuje logičku povezanost lokacija ustanova i korisnika na privatnu mrežu CARNET putem koje pristupaju dodijeljenim resursima unutar CARNET-ovih podatkovnih centara, Internetu i svim ostalim servisima u javnom i privatnom oblaku.



Slika 1.

Slika 2. prikazuje planirani SD-WAN mrežni nadsloj za lokacije ustanova uključene u projekt, korisničke prometne tokove te komunikaciju između komponenti sustava i upravljačke jedinice.



Slika 2.

3. Tehničko-funkcionalni zahtjevi Sustava

Zahtijevane funkcionalnosti Sustava podijeljene su na opće, sigurnosne, integracijske i izvještajno-analitičke karakteristike (tablice se nalaze ispod kao i u Prilogu 1. Dokumentacije).

U Tablici 1. opisane su opće karakteristike Sustava koje je potrebno podržati kroz Sustav za upravljanje i nadzor pristupne mreže.

Opće karakteristike Sustava	
1	Sustav mora podržavati funkcionalnost stvaranja mrežnog nadsloja nad postojećim širokopojasnim pristupnim vezama i mrežnim tehnologijama u privatnoj mreži CARNET (IP/MPLS) pružajući sigurnu (enkriptiranu) komunikaciju s kraja na kraj između: • svake lokacije ustanova pojedinačno i CARNET podatkovnih centara, • svih lokacija koje pripadaju istoj ustanovi, • više lokacija različitih ustanova ovisno o potrebama
2	Sustav mora podržavati funkcionalnost centraliziranog definiranja svih politika uključujući i sigurnosne politike
3	Sustav mora podržavati funkcionalnost orkestracije svih postavki i usluga kroz sve uređaje sustava putem jedinstvenog centralnog web sučelja. Sustav za orkestraciju, upravljanje, nadzor i analitiku mora se implementirati redundantno lokalno na dvije lokacije CARNET-ovih podatkovnih centara na lokacijama Jastrebarsko-PCK i Osijek (on-premise high availability deployment)
4	Sustav mora podržavati funkcionalnost “Zero Touch” konfiguracije s ciljem brzog deploymenta uređaja (instalacija svih mrežnih uređaja i spajanje na sustav za upravljanje i nadzor bez prethodnog spajanja na uređaj i promjene tvorničkih postavki uređaja)
5	Sustav mora podržavati RBAC (role-based access control) metodu za kreiranje uloga više mrežnih administratora i administratorskih grupa za upravljanje i nadzor: • cijelim sustavom novog mrežnog rješenja, • dijelom sustava dodijeljenim pojedinim lokacijama ustanova (jedna ili više lokacija ustanova)
6	Sustav mora podržavati podjelu svih postavki uređaja na lokacijama ustanova u dvije skupine: • postavke kojima upravljaju mrežni administratori zaduženi za jednu ili više ustanova i globalni administrator Sustava, • postavke kojima upravlja isključivo globalni administrator Sustava

7	Sustav mora podržavati funkcionalnost dinamičkog upravljanja prometom (usmjeravanje i prioritizacija) ovisno o: • aplikacijama (application aware routing i application policy based forwarding), • prepoznatim grupama korisnika
8	Sustav mora podržavati funkcionalnost prioritizacije prepoznatog prometa i usmjeravanja prepoznatog prometa na: • centralne hub uređaje (Spoke/Branch <-> Hub <-> internet), • direktno na internet (Spoke/Branch <-> internet). Usmjeravanje prometa mora biti simetrično, što znači da za određeni tip prometa odlazno i dolazno (logičko) sučelje mora biti isto
9	Sustav mora podržavati funkcionalnost uključivanje/isključivanje sigurnosne inspekcije ovisno o: • aplikacijama, • prepoznatim grupama korisnika
10	Sustav za upravljanje i nadzor mora biti proširiv s minimalno 50 dodatnih SD-WAN uređaja u odnosu na ovom nabavom predviđenu količinu opreme zbog budućih potreba
11	Sustav mora podržavati funkcionalnost povezivanja sigurnim tunelima svih lokacija koje pripadaju pojedinoj ustanovi u smislu distribuirane infrastrukture svake ustanove u jedinstvenu virtualnu domenu uz pružanje QoS i sigurnosnih usluga na SD-WAN uređajima
12	Sustav mora podržavati funkcionalnost povezivanja svake ustanove u sustavu sigurnim tunelima s informacijskim resursima podatkovnih centara (javnim i privatnim servisima u oblaku) uz pružanje QoS i sigurnosnih usluga na SD-WAN uređajima
13	Nedostupnost sustava za upravljanje i nadzor ne prekida prometne tokove konfiguriranih SD-WAN uređaja
14	Sustav mora podržavati centralizirano upravljanje i nadzor svih ili odabranih elemenata sustava, njihovih postavki, konfiguriranih usluga i sigurnosnih funkcija putem jedinstvenog web sučelja

Tablica 1.

U Tablici 2. opisane su sigurnosne karakteristike Sustava koje je potrebno podržati kroz Sustav za upravljanje i nadzor pristupne mreže.

Sigurnosne karakteristike Sustava	
1	Sustav mora podržavati funkcionalnost blokiranja ili propuštanja mrežnog prometa na 3. i 4. sloju OSI složaja (layer 3 i layer 4 stateful firewall)
2	Sustav mora podržavati funkcionalnost blokiranja ili propuštanja pojedinih aplikacija na 7. sloju OSI složaja (layer 7 application firewall)

3	Sustav mora podržavati funkcionalnost IDS (intrusion detection system) za analizu mrežnog prometa i detekciju malicioznog mrežnog prometa
4	Sustav mora podržavati funkcionalnost IPS (intrusion prevention system) za analizu mrežnog prometa, detekciju i blokiranje mrežnog prometa, ovisno o vrsti prometa koji sustav detektira kao maliciozni
5	Sustav mora podržavati funkcionalnost SSL (*secure socket layer*) inspekcije
6	Sustav mora podržavati funkcionalnost blokiranja dolaznog i odlaznog prometa prema IP adresi s lošom reputacijom, URL poveznici s lošom reputacijom i internet domeni (FQDN) s lošom reputacijom
7	Sustav mora podržavati funkcionalnost kreiranja i primjene crnih i bijelih lista za IP adrese, URL poveznice i internet domene (FQDN)
8	Sustav mora podržavati funkcionalnost antivirusne inspekcije
9	Sustav mora podržavati funkcionalnost antimalware inspekcije
10	Sustav mora podržavati secure web gateway funkcionalnost
11	Sustav mora podržavati funkcionalnost ažurne lokalne baze hash algoritama uz redovito dnevno osvježavanje
12	Sustav mora podržavati funkcionalnost ažurne lokalne baze poznatih signatura malicioznih programa radi detekcije istih u mrežnom prometu (npr. putem yara pravila) uz redovito osvježavanje sa novootkrivenim ugrozama
13	Sustav mora podržavati funkcionalnost detekcije anomalija u mrežnom prometu koje mogu upućivati na kompromitaciju ili pokušaj kompromitacije kao što su eksfiltracija podataka, C2 beaconing i agresivno mrežno skeniranje
14	Sustav mora podržavati VPN (*Virtual Private Network*) funkcionalnost sigurnog udaljenog pristupa kroz enkriptirani tunel za ostvarivanje pristupa informacijskim resursima ustanova korištenjem AAI identiteta
15	VPN klijentska aplikacija mora biti javno dostupna za MS Windows, MacOS i Linux operativne sustave
16	Sustav mora podržavati ZTNA (*Zero Trust Network Access*) funkcionalnost sigurnog udaljenog pristupa kroz enkriptirani tunel za ostvarivanje pristupa informacijskim resursima ustanova korištenjem AAI identiteta
17	ZTNA klijentska aplikacija mora biti javno dostupna za MS Windows, MacOS i Linux operativne sustave
18	ZTNA klijenska aplikacija mora imati funkcionalnost dohvaćanja Kubernetes i OpenStack tagova

Tablica 2.

U Tablici 3. opisane su integracijske karakteristike Sustava, nužne za omogućavanje komunikacije s postojećim sustavima koje koristi Naručitelj. Ako u trenutku podnašanja ponude ne postoji podrška za funkcionalnosti navedene u Tablici 3., odabrani Ponuditelj se obvezuje razviti navedenu funkcionalnost.

Integracijske karakteristike Sustava	
1	Administratori sustava posjeduju korisnički račun u AAI@EduHr sustavu. Ponuditelj mora integrirati rješenje s autentikacijskom i autorizacijskom AAI@EduHr infrastrukturom putem SAML2 ili OAuth2 protokola u svrhu pristupa mrežnih administratora na Sustav te za udaljeno povezivanje VPN i ZTNA klijenata na mrežu ustanove. Ovisno o vrijednosti dogovorenog atributa autenticiranom korisniku dodjeljuju se read-only ili read-write prava koja se dodatno reguliraju putem RBAC mehanizma (sustav je detaljno opisan na poveznici https://www.aaiedu.hr/)
2	Ponuditelj mora integrirati rješenje s CARNET-ovim NetBox sustavom koristeći API pozive u svrhu dohvata svih podataka potrebnih za *Zero Touch* deployment (sustav je detaljno opisan na poveznici https://docs.netbox.dev/en/stable/)
3	Ponuditelj mora integrirati rješenje s CARNET-ovim RT (Request Tracker) ticketing sustavom koristeći REST API pozive u svrhu konfigurabilne pretrage/otvaranja/izmjene/zatvaranja tiketa vezanih za upravljanje incidentima i promjene stanja nadziranih elemenata sustava (sustav je detaljno opisan na poveznici https://bestpractical.com/request-tracker)
4	Sustav mora podržavati funkcionalnost streaming telemetrije bazirane na otvorenim protokolima
5	Sustav mora podržavati funkcionalnost integracije sa SIEM sustavima (syslog, json)
6	Sustav mora podržavati funkcionalnost integracije sa custom threat intel feedovima
7	Sustav mora podržavati funkcionalnost integracije s drugim sustavima kroz izvoz logova i opisa mrežnog prometa u modernim formatima (json, cef i syslog)
8	Sustav mora podržavati funkcionalnost integracije sa drugim sustavima kroz REST API pozive za sve upravljačko nadzorne funkcionalnosti

Tablica 3.

U Tablici 4. opisane su izvještajno-analitičke karakteristike Sustava.

Sustav za orkestraciju, upravljanje i nadzor, kroz web sučelje, mora omogućiti napredne analitičke i izvještajne značajke koje pružaju uvid u performanse i sigurnost mreže u realnom vremenu, te povijesni pregled istih za minimalno zadnjih 5 godina, kako bi osigurali brzo dijagnosticiranje problema i optimizaciju performansi mreže.

Izvještajno-analitičke karakteristike Sustava	
1	Sustav mora podržavati vidljivost količine prometa, broja paketa po sekundi, grešaka (errora) i discarda na svim sučeljima odabranog uređaja, u realnom vremenu te grafički prikaz povjesnih podataka
2	Sustav mora podržavati funkcionalnost generiranja preddefiniranih i prilagođenih izvještaja na temelju prikupljenih povijesnih podatatka, po svim ili

	odabranim elementima sustava, njihovim postavkama, konfiguriranim uslugama i sigurnosnim funkcijama
3	Sustav mora podržavati funkcionalnost generiranja preddefiniranih i prilagođenih izvještaja o povijesnom pregledu dostupnosti uređaja, potrošnji mrežnog prometa (po sučeljima) te latenciji i gubitnicima za pojedinu lokaciju (per site), za odabrane lokacije (multi-site) i za sve lokacije u Sustavu
4	Sustav mora podržavati funkcionalnost analitike koreliranjem prikupljenih povijesnih (minimalno 5 godina) podataka s odabranih elemenata sustava, njihovih postavki, konfiguriranih usluga i sigurnosnih funkcija
5	Sustav mora podržavati funkcionalnost predikcije potrošnje mrežnog prometa na temelju korelacije povijesnih podataka
6	Sustav mora podržavati funkcionalnost prepoznavanja mrežnih i sigurnosnih anomalija i upravljanja incidentima
7	Sustav mora podržavati vidljivost prometa po aplikacijama i grupama korisnika po lokaciji (per-site) u realnom vremenu
8	Sustav mora podržavati funkcionalnost generiranja planiranih (scheduled) izvještaja
9	Sustav mora podržavati funkcionalnost generiranja izvještaja na zahtjev (ad-hoc)
10	Sustav mora podržavati funkcionalnost izrade predefiniranih i prilagođenih predložaka izvješća
11	Sustav mora podržavati funkcionalnost izvoza izvještaja u formatima CSV, PDF, XLS i slanjem obavijesti putem e-pošte (kroz sučelje sustava)

Tablica 4.

Opće i specifične tehničko-funkcionalne karakteristike *SD-WAN* uređaja opisane su u Tablici 5.

Karakteristike Sustava koje su podržane na svakom SD-WAN uređaju	
1	Uređaj mora imati integriranu podršku usmjeravanje, preklapanje i sigurnost
2	Uređaj mora podržavati virtualizaciju WAN sučelja na Layeru 2 koristeći 802.1Q tagiranje (logički uplink). Funkcionalnost dinamičkog upravljanja prometom mora biti podržan nad tako kreiranim logičkim uplink-om
3	Uređaj mora podržavati dual stack (IPv4 i IPv6) funkcionalnost. Sve (sigurnosne) funkcionalnosti za IPv4 protokol moraju biti podržane i za IPv6 protokol
4	Uređaj mora podržavati DHCPv4 i DHCPv6 server i relay funkcionalnost
5	Uređaj mora podržavati NAT funkcionalnost: • NAT 1:1, • PAT 1:N
6	Uređaj mora podržavati funkcionalnost NAT logiranja na vanjski syslog server.
7	Uređaj mora podržavati Layer 3 usmjeravanje za IPv4 i IPv6 protokol: • statičko usmjeravanje, • BGP, • OSPF

8	Uređaj mora imati mogućnost postavljanja BGP community-a na prefikse koje oglašava preko BGP-a
9	Uređaj mora imati QoS funkcionalnost: • traffic policing, • traffic shaping, • per-flow queueing
10	Uređaj mora podržavati minimalno 1000 enkriptiranih tunela po SD-WAN uređaju između svih SD-WAN uređaja
11	Uređaj mora podržavati third-party primopredajnike i njihovom se ugradnjom u uređaje ne utječe na garanciju/održavanje uređaja
12	Uređaj mora podržavati mjerenje kvalitete veze/servisa na uplink sučelju ((jitter, packet loss, latency)
13	Uređaj mora imati funkcionalnost redundantnog povezivanja linkova i usmjeravanja ovisno o tipu prometa preko pojedinog linka
Sigurnosni SD-WAN uređaj TIP1	
Tehničko-funkcionalne karakteristike uređaja	
1	Uređaj je moguće ugraditi u 19” komunikacijski ormar i zauzima maksimalno 1U (pomoću kompleta za montažu ili korištenjem police)
2	Uređaj ima funkcionalnost automatske instalacije na lokaciji bez potrebe bilo kakve dodatne konfiguracije na lokaciji (Zero Touch Deployment)
3	Uređaj ima minimalno 2 SFP sučelja minimalne brzine 1Gbit/s
4	Uređaj ima minimalno 4 RJ45 sučelja minimalne brzine 1Gbit/s
5	Uređaj ima minimalno **200Mbit/s** propusnost sa uključenim sigurnosnim funkcijama*
6	Uređaj mora podržavati minimalno 100K istovremenih sesija
7	Uređaj mora podržavati minimalno 5K novih sesija po sekundi
Sigurnosni SD-WAN uređaj TIP2	
Tehničko-funkcionalne karakteristike uređaja	
1	Uređaj je moguće ugraditi u 19” komunikacijski ormar i zauzima maksimalno 1U (pomoću kompleta za montažu ili korištenjem police)
2	Uređaj ima funkcionalnost automatske instalacije na lokaciji bez potrebe bilo kakve dodatne konfiguracije na lokaciji (Zero Touch Deployment)
3	Uređaj ima minimalno 4 SFP+ sučelja minimalne brzine 10Gbit/s
4	Uređaj ima minimalno 4 RJ45 sučelja minimalne brzine 10Gbit/s
5	Uređaj ima minimalno **2Gbit/s** propusnost sa uključenim sigurnosnim funkcijama*
6	Uređaj mora podržavati minimalno 1,5M istovremenih sesija
7	Uređaj mora podržavati minimalno 75K novih sesija po sekundi
Sigurnosni SD-WAN uređaj TIP3	
Tehničko-funkcionalne karakteristike uređaja	
1	Uređaj je moguće ugraditi u 19” komunikacijski ormar i zauzima maksimalno 2U (pomoću kompleta za montažu ili korištenjem police)
2	Uređaj ima funkcionalnost automatske instalacije na lokaciji bez potrebe bilo kakve dodatne konfiguracije na lokaciji (Zero Touch Deployment)

3	Uređaj ima dvostruku (1+1 redundancija) jedinicu za napajanje
4	Uređaj je moguće upariti s istovjetnim uređajem u active-active i active-passive načinu rada radi postizanja visoke dostupnosti prema WAN i LAN strani
5	Uređaj ima minimalno 8 SFP+ sučelja minimalne brzine 10Gbit/s
6	Uređaj ima minimalno 4 RJ45 sučelja minimalne brzine 10Gbit/s
7	Uređaj ima minimalno **5Gbit/s** propusnost sa uključenim sigurnosnim funkcijama*
8	Uređaj mora podržavati minimalno 4M istovremenih sesija
9	Uređaj mora podržavati minimalno 200K novih sesija po sekundi
Sigurnosni SD-WAN uređaj TIP4	
Tehničko-funkcionalne karakteristike uređaja	
1	Uređaj je moguće ugraditi u 19” komunikacijski ormar i zauzima maksimalno 2U (pomoću kompleta za montažu ili korištenjem police)
2	Uređaj ima funkcionalnost automatske instalacije na lokaciji bez potrebe bilo kakve dodatne konfiguracije na lokaciji (Zero Touch Deployment)
3	Uređaj ima dvostruku (1+1 redundancija) jedinicu za napajanje
4	Uređaj je moguće upariti s istovjetnim uređajem u active-active i active-passive načinu rada radi postizanja visoke dostupnosti prema WAN i LAN strani
5	Uređaj ima minimalno 4 QSFP28 sučelja minimalne brzine 100Gbit/s
6	Uređaj ima minimalno 8 SFP+ sučelja minimalne brzine 10Gbit/s
7	Uređaj ima minimalno **10Gbit/s** propusnost sa uključenim sigurnosnim funkcijama*
8	Uređaj mora podržavati minimalno 8M istovremenih sesija
9	Uređaj mora podržavati minimalno 400K novih sesija po sekundi

Tablica 5.

*Sigurnosne funkcije uz SDWAN uključuju Statefull Firewall, Layer 7 Next Generation Firewall i Application Visibility, IPS/IDS, SSL inspekciju, web filtering, antivirus i antimalware.

Specifične tehničko-funkcionalne karakteristike primopredajnika koji se ugrađuju u SD-WAN uređaje opisane su u Tablici 6.

Primopredajnik TIP1	
Tehničko-funkcionalne karakteristike primopredajnika	
1	Primopredajnik mora biti SFP industrijskog formata (1 Gbit/s)
2	Primopredajnik mora podržavati jednomodnu optiku (SMF) valne duljine 1310nm
3	Primopredajnik mora podržavati minimalnu duljinu OSx optičkog kabela od 10km
4	Primopredajnik mora podržavati kabele s LC tipom konektora (duplex)
5	Primopredajnik mora imati DOM ili DDM funkcionalnost
6	Primopredajnik mora biti podržan na sljedećoj opremi: Uređaj TIP 1

Primopredajnik TIP2	
Tehničko-funkcionalne karakteristike primopredajnika	
1	Primopredajnik mora biti SFP industrijskog formata (1 Gbit/s)
2	Primopredajnik mora podržavati jednomodnu optiku (SMF) valne duljine: TX: 1310 nm, RX: 1490 nm
3	Primopredajnik mora podržavati minimalnu duljinu OSx optičkog kabela od 10km
4	Primopredajnik mora podržavati rad s jednim optičkim vlaknom (LC tip konektora)
5	Primopredajnik mora imati DOM ili DDM funkcionalnost
6	Primopredajnik mora biti podržan na sljedećoj opremi: Uređaj TIP1
Primopredajnik TIP3	
Tehničko-funkcionalne karakteristike primopredajnika	
1	Primopredajnik mora biti SFP+ industrijskog formata (10 Gbit/s)
2	Primopredajnik mora podržavati jednomodnu optiku (SMF) valne duljine 1310nm
3	Primopredajnik mora podržavati minimalnu duljinu OSx optičkog kabela od 10km
4	Primopredajnik mora podržavati kabele s LC tipom konektora (duplex)
5	Primopredajnik mora imati DOM ili DDM funkcionalnost
6	Primopredajnik mora biti podržan na sljedećoj opremi: Uređaj TIP 2, TIP3, TIP4
Primopredajnik TIP4	
Tehničko-funkcionalne karakteristike primopredajnika	
1	Primopredajnik mora biti SFP+ industrijskog formata (10 Gbit/s)
2	Primopredajnik mora podržavati jednomodnu optiku (SMF) valne duljine: TX: 1310 nm, RX: 1490 nm
3	Primopredajnik mora podržavati minimalnu duljinu OSx optičkog kabela od 10km
4	Primopredajnik mora podržavati rad s jednim optičkim vlaknom (LC tip konektora)
5	Primopredajnik mora imati DOM ili DDM funkcionalnost
6	Primopredajnik mora biti podržan na sljedećoj opremi: Uređaj TIP 2, TIP3, TIP4
Primopredajnik TIP5	
Tehničko-funkcionalne karakteristike primopredajnika	
1	Primopredajnik mora biti QSFP28 industrijskog formata (100 Gbit/s)
2	Primopredajnik mora podržavati jednomodnu optiku (SMF) valnih duljina: 1295nm, 1300nm, 1304nm, 1309nm
3	Primopredajnik mora podržavati minimalnu duljinu OSx optičkog kabela od 10km
4	Primopredajnik mora podržavati kabele s LC tipom konektora (duplex)
5	Primopredajnik mora imati DOM ili DDM funkcionalnost
6	Primopredajnik mora biti podržan na sljedećoj opremi: Uređaj TIP 4

Primopredajnik TIP6	
Tehničko-funkcionalne karakteristike primopredajnika	
1	Primopredajnik mora biti QSFP28 industrijskog formata (100 Gbit/s)
2	Primopredajnik mora podržavati višemodnu optiku (MMF) valne duljine 844 – 863 nm
3	Primopredajnik mora podržavati minimalnu duljinu OM4 optičkog kabela od 100m
4	Primopredajnik mora podržavati kabele s LC tipom konektora (duplex)
5	Primopredajnik mora imati DOM ili DDM funkcionalnost
6	Primopredajnik mora biti podržan na sljedećoj opremi: Uređaj TIP 4

Tablica 6.

Dijagnostika i sistemsko logiranje

U sklopu nadzora mreže, unutar sustava za upravljanje i nadzor moraju biti omogućene sljedeće funkcionalnosti:

- Integracija s vanjskim *syslog* serverom na kojeg će se slati syslog zapisi,
- Logiranje sistemskih događaja sa svih uređaja instaliranih u sklopu mrežnog rješenja,
- Logiranje zapisa o mrežnim sesijama vezanih za NAT logiranje.

4. Jamstvo

Odabrani Ponuditelj je nakon implementacije elemenata aktivne mrežne infrastrukture obvezan isporučiti jednogodišnje jamstvo kvalitete izvedenih radova na ugradnji opreme u roku od 30 dana od dana potpisivanja zadnjeg primopredajnog zapisnika. Jamstvo kvalitete izvedenih radova uključuje postavljanje svih komponenti centralnog sustava i SD-WAN uređaja u komunikacijske ormare te povezivanje svih komponenti sustava.

Odabrani Ponuditelj jamči za ispravnost opreme i cjelokupnog sustava instaliranog na ustanovama ili podatkovnom centru Naručitelja u razdoblju od minimalno 120 mjeseci od predaje opreme i sustava Naručitelju. Odabrani ponuditelj je dužan jamstvo izdati na rok od 120 mjeseci od dana potpisivanja zadnjeg primopredajnog zapisnika za implementaciju SDWAN sustava.

Za vrijeme jamstvenog roka odabrani Ponuditelj je dužan poduzeti sve radnje i popravke, uključivo nužnu i sigurnosnu nadogradnju sustava (uključujući softver bilo koje komponente sustava) koje su potrebne da bi se otklonili nedostatci u funkcioniranju opreme i sustava, te sigurnosne ranjivosti i sigurnosne propuste. Radnje koje poduzima odabrani Ponuditelj za vrijeme jamstvenog roka odnose se isključivo na otklanjanje nedostataka, sigurnosnih ranjivosti i sigurnosnih propusta, te neispravnost u radu opreme i sustava za vrijeme jamstvenog roka.

Za slučaj da se kvar i/ili nedostatak na opremi i/ili sustavu ne može otkloniti popravkom opreme te je nužno izvršiti zamjenu, odabrani Ponuditelj je dužan izvršiti zamjenu s onom opremom koja je istih ili boljih karakteristika od opreme koja se mijenja, na način da nova oprema udovoljava minimalnim karakteristikama propisanim tehničkim specifikacijama. Zamjenu pristupne mrežne opreme odabrani Ponuditelj će izvršiti u roku od jednog radnog dana od prijave kvara. Ako za isto postoji opravdan razlog, Naručitelj je na zahtjev odabranog Ponuditelja ovlašten produžiti prethodno navedeni rok.

Odabrani Ponuditelj ne odgovara za one nedostatke opreme i sustava koji su nastali krivnjom Naručitelja i/ili osoba za koje Naručitelj odgovara ili su posljedica više sile ili drugih nepredviđenih okolnosti. Navedeno primjerice uključuje nepravilno rukovanje opremom, propust Naručitelja i/ili korisnika opreme da osigura ispravne uvjete u prostoru u kojem je oprema smještena i sl.

Odabrani Ponuditelj je dužan predati Naručitelju jamstva za ispravnost opreme, točnije jamstvene listove izdane od strane proizvođača opreme te u tom slučaju Naručitelj može ostvariti svoja prava sukladno čl.423. Zakona o obveznim odnosima (NN 35/05, 41/08, 125/11, 78/15, 29/18) u roku od 30 dana od dana potpisa zadnjeg primopredajnog zapisnika.

Troškove otklanjanja nedostataka i/ili kvarova za vrijeme jamstvenog roka u cijelosti snosi odabrani Ponuditelj.

Naručitelj će u svakoj ustanovi imenovati osobu (mrežnog administratora), koja će biti ovlaštena prijavljivati neispravnosti u radu ili kvarove opreme. Prijava od strane ustanova se vrši CARNET-ovom Helpdesku.

Odabrani Ponuditelj za vrijeme jamstvenog roka mora omogućiti prijavu problema i kvarova radnim danima u Republici Hrvatskoj (ponedjeljak–petak, osim blagdana i državnih praznika) od 8h do 20h, s odzivom od 2h od trenutka prijave. Ako je prijava zaprimljena do 15h tekućeg dana tada je odabrani Ponuditelj dužan započeti s analizom i rješavanjem problema isti dan, a inače je dužan započeti s rješavanjem problema sljedeći radni dan.

Odabrani Ponuditelj je obavezan oformiti sustav podrške Naručitelju na sljedeći način:

- Osigurati *Helpdesk* sustav za ustanove uključene u projekt. *Helpdesk* pruža podršku Naručitelju koji je globalni administrator sustava. Navedena podrška odnosi se isključivo na otklanjanje nedostataka i neispravnosti u radu isporučenog sustava i opreme,
- Osigurati prijavu kvara i/ili neispravnosti u radu te otklanjanje nedostataka (ako je moguće) putem telefona, elektronske pošte, Web stranice Helpdesk sustava,
- Osigurati, prema potrebi, izlazak ovlaštenog tehničara na lokaciju ustanove.

Ako se problem može otkloniti udaljenim pristupom tada nije obavezno da djelatnik odabranog Ponuditelja izlazi na lokaciju, ali kvar mora biti otklonjen u roku ne dužem od definiranog vremena potrebnog za zamjenu opreme. Iznimno se za lokacije Naručitelja koje imaju otežan ili ograničen pristup, vrijeme odziva može produžiti zbog objektivne situacije s terena (neprohodne prometnice, vozni red trajekta i slično). Za takve lokacije odabrani Ponuditelj ima obvezu zamjene opreme ili dolaska na lokaciju u najkraćem mogućem roku, dogovorenog sukladno odobrenju Naručitelja.

Naručitelj će svakoj ustanovi osigurati pristup CARNET mreži, a time i Internetu. Ako postoji problem s povezanosti ustanove na CARNET mrežu, tada će Naručitelj otkloniti poteškoću s povezanosti prije nego odabrani Ponuditelj krene s rješavanjem problema. U tom slučaju se vrijeme odziva odnosno otklanjanje problema računa tek od trenutka kad je potvrđeno kako je s povezanosti na CARNET mrežu sve u redu.

5. Edukacija

Uz implementaciju aktivne mrežne infrastrukture odabrani, Ponuditelj je dužan administratorima zaduženim za pružanje tehničke podrške imenovanih od strane ustanova u projektu i djelatnicima CARNET-a osigurati edukaciju i edukacijske materijale. Sve edukacije se trebaju provesti u obliku interaktivnih radionica na hrvatskom jeziku. Osim izvođenja same edukacije, odabrani Ponuditelj je dužan izraditi i dostaviti Plan provedbe edukacije te lektorirane edukacijske materijale – digitalni priručnik, video upute i materijale za radionice. Svim izrađenim edukacijskim materijalima CARNET će imati pravo raspolagati neograničeno i isključivo. Odabrani Ponuditelj se obvezuje provesti 12 trodnevnih cjelodnevnih radionica, od kojih će se 10 radionica provesti uživo u većim gradovima, a dvije radionice provesti će se u formi webinara. Svaka radionica uživo imati će maksimalno 25 polaznika, a webinari neće imati ograničenje broja polaznika. CARNET će osigurati prostore za održavanje radionica uživo, a troškovi putovanja i/ili smještaja polaznika biti će osigurani izvan obuhvata ove nabave. Sve ostale troškove provedbe radionica snosi odabrani Ponuditelj.

6. Usluge instalacije i konfiguracije

Odabrani Ponuditelj je dužan usluge instalacije i konfiguracije sve opreme definirane u sklopu ovog postupka nabave, uključiti u cijenu ponude. Inicijalna konfiguracija namijenjena pojedinoj ustanovi definirat će se u suradnji s Naručiteljem nakon potpisivanja ugovora.

U sklopu instalacije opreme, odabrani Ponuditelj je dužan odraditi lijepljenje naljepnica. Odabrani Ponuditelj će izraditi naljepnice prema standardima definiranim od strane Naručitelja te ih postaviti prilikom instalacije na elemente sustava prema uputama Naručitelja.

Prilikom instalacije i konfiguracije opreme na ustanovama, odabrani Ponuditelj je dužan odraditi integraciju lokalne računalne mreže s novo implementiranom mrežnom opremom i osigurati da svi prethodno korišteni servisi na ustanovama budu funkcionalni i nakon završetka instalacije nove opreme, osim ako to nije drugačije dogovoreno s Naručiteljem i predstavnikom ustanove.

7. Dinamika implementacije

Implementacija softverski definiranog mrežnog pristupnog sustava sa sigurnosnom komponentom bit će podijeljena u tri faze. Početkom faze smatra se datum označen u nalogu za pojedinu fazu poslanom na unaprijed dogovorenu elektroničku adresu.

S obzirom na velik broj lokacija rasprostranjenih po cijeloj Hrvatskoj, odabrani Ponuditelj se obvezuje da će u roku 30 dana od potpisivanja ugovora dostaviti plan projektnih aktivnosti vezanih uz instalaciju i konfiguraciju mrežne infrastrukture. Nakon dostave, Naručitelj i odabrani Ponuditelj usuglašavaju predloženi terminski plan. Ako dođe do probijanja terminskog plana zbog krivnje odabranog Ponuditelja isti će plaćati kaznu definiranu u sklopu ugovora, a ako dođe do probijanja terminskog plana zbog krivnje Naručitelja ili trećih strana koje sudjeluju u projektu (na primjer ustanova) tada je moguće produljiti rok za završetak projektnih aktivnosti za onoliko dana koliko je uzrokovano zbog krivnje ili nepridržavanja plana Naručitelja ili trećih strana.

U prvoj fazi provesti će se uspostava sustava za orkestraciju, upravljanje i nadzor sigurnosne SD-WAN mreže sa svim komponentama uključujući redundanciju i integraciju sustava za orkestraciju, upravljanje i nadzor sigurnosne SD-WAN mreže sa sustavima koje koristi Naručitelj (Tablica 3.) Rok trajanja prve faze je 60 dana od dana naznačenog u nalogu izdanog od strane Naručitelja.

U drugoj fazi provesti će se implementacija SD-WAN uređaja sa osnovnim funkcionalnostima po lokacijama ustanova. U ovoj fazi provesti će se postavljanje SD-WAN uređaja na novim lokacijama i zamjena pristupne opreme na postojećim lokacijama SD-WAN uređajima te uspostava istovjetne funkcionalnosti kao na postojećoj opremi, što uključuje Layer 3 usmjeravanje, NAT, DHCP i ACL (tamo gdje i sada postoji ta funkcionalnost). Postavljanje i zamjena uređaja bit će podijeljena u 3 slota po 30 dana sa razmakom od minimalno 7 dana između slotova ili više ako Naručitelj tako odluči i odvijat će se u redovnom radnom vremenu. Odabrani Ponuditelj će u dogovoru sa Naručiteljem povući postojeću pristupnu opremu sa lokacija ustanova tamo gdje je ona u vlasništvu Naručitelja te će navedenu opremu dostaviti na centralnu lokaciju Naručitelja. Odabrani Ponuditelj mora osigurati tehničku podršku koja će omogućiti otklanjanje svih smetnji na Sustavu u roku jednog radnog dana, prema potrebi korištenjem udaljenog pristupa ili intervencijama na svim lokacijama ustanova i Naručitelja gdje su implementirani SD-WAN uređaji. Početkom pojedinog slota u drugoj fazi se smatra datum označen u nalogu za pojedini slot (ukupno tri naloga u drugoj fazi). U ovoj fazi odabrani Ponuditelj dužan je izraditi i dostaviti sve edukacijske materijale. Za vrijeme trajanja druge faze administratori zaduženi za tehničku podršku na ustanovama neće imati pristup SD-WAN sustavu. Za izradu i dostavu svih edukacijskih materijala izdati će se poseban nalog u sklopu druge faze, a rok primopredaje određen je rokom završetka trećeg slota u drugoj fazi.

U trećoj fazi provoditi će se implementacija i prilagodba svih dostupnih naprednih funkcionalnosti na ustanovama. Napredne funkcionalnosti bit će podijeljene na globalne (kojima će kroz implementaciju predložaka i specifične zahtjeve ustanova upravljati

djelatnici CARNET-a) i lokalne (za pojedinu ustanovu koje će biti implementirane davanjem prava pristupa na sustav administratorima zaduženim za tehničku podršku na ustanovama). Ustanove će imati različite razine kompleksnosti implementacije i kompetencija. Odabrani ponuditelj mora osigurati tehničku podršku koja će do kraja trajanja Ugovora omogućiti implementaciju i prilagodbu naprednih funkcionalnosti kao i otklanjanje svih smetnji na Sustavu u roku jednog radnog dana, prema potrebi korištenjem udaljenog pristupa ili intervencijama na svim lokacijama ustanova i Naručitelja gdje su implementirani SD-WAN uređaji. Početkom treće faze se smatra datum označen u nalogu za početak, dok je rok trajanja treće faze do kraja trajanja projekta. Aktivnost treće faze za pojedinu lokaciju ustanovu smatrat će se odrađenom definiranjem primopredajnog zapisnika.

U ovoj fazi odabrani Ponuditelj dužan je odraditi edukacije administratora na ustanovama i djelatnika CARNET-a. Za održavanje edukacija izdati će se poseban nalog u sklopu treće faze, a rok je određen završetkom treće faze.

Rokovi izraženi u ovom dokumentu počinju teći početkom prvoga sata prvoga dana i završava istekom posljednjeg sata zadnjeg dana toga roka. Državni blagdani, subote i nedjelje ne utječu na početak i tijek roka. Ako posljednji dan roka pada na državni blagdan, subotu ili nedjelju, rok istječe protekom posljednjeg sata sljedećeg radnog dana. Uslijed objektivnih okolnosti, a na zahtjev Ponuditelja, Naručitelj može produžiti rokove.

8. Obveze odabranog Ponuditelja

U sklopu projekta obveze odabranog Ponuditelja su:

- U koordinaciji s Naručiteljem izrada vremenskog plana aktivnosti za svaku lokaciju ustanovu i za projekt u cjelini,
- Sudjelovanje na redovitim koordinacijama sukladno dogovoru s Naručiteljem,
- Vođenje projekta,
- Isporuka opreme na lokacije navedene u Dokumentaciji,
- Implementacija elementa aktivne mrežne opreme po svakoj lokaciji navedenoj u Dokumentaciji po pravilima struke i pozitivnih propisa,
- Instalacija i konfiguracija aktivne mrežne opreme iz ovog projekta od strane ovlaštenih i stručnih osoba odabranog Ponuditelja u skladu sa zahtjevima Naručitelja,
- Testiranje osnovne funkcionalnosti opreme na svakoj lokaciji ustanovi i na lokacijama Naručitelja,
- Isporuka evidencije serijskih brojeva svih komponenti sustava instaliranih po pojedinoj lokaciji ustanove, u digitalnom formatu (.xls),
- Nabava i ugradnja UTP prespojih kabela za povezivanje unutar istog komunikacijskog razdjelnika. UTP kabeli moraju biti 4 parični Cat.6A (klasa EA) prema normi HRN EN 50173:1 ili jednakovrijednoj,
- Nabava i ugradnja jednomodnih (Singlemode) i višemodnih (Multimode) prespojnih svjetlovodnih kabela za povezivanje unutar istog komunikacijskog ormara s vrstama konektora sukladnim tipovima primopredajnika navedenim u tablici tehničko-funkcionalnih zahtjeva (Tablica 6.),
- Edukacija korisnika,
- Podrška Naručitelju,
- Integracija lokalne računalne mreže lokacija ustanova s novo implementiranom mrežnom opremom,
- Nabava i postavljanje oznaka vidljivosti EU sufinanciranja,
- Izrada upute o konfiguriranju sustava za potrebe provođenja demo testiranja.

8.1. Obveze stručnjaka za implementaciju ponuđenog rješenja

Stručnjak za implementaciju ponuđenog rješenja je osoba koja na zahtjev Naručitelja za vrijeme trajanja ugovora boravi na lokaciji Naručitelja.

- Središnja je kontakt osoba za pitanja i poteškoće prilikom implementacije aktivne mrežne opreme nabavljene u sklopu ove nabave, te obavlja sljedeće poslove:
- U suradnji s Naručiteljem predlaže dizajn i početnu konfiguraciju mreže ustanove,
- Uklanja mrežne poteškoće prilikom implementacije aktivne mrežne opreme na ustanovama,

- Pruža podršku prilikom implementacije aktivne mrežne opreme na lokaciji i integracije s postojećom lokalnom računalnom mrežom ustanove,
- Komunicira s razvojnim timom proizvođača vezano za razvoj, testiranje i implementaciju traženog sustava i njegovih funkcionalnosti,
- Razrađuje procedure za nadogradnju mrežne opreme,
- Testira mrežu i opremu za potrebe verifikacije ispravnosti rada iste.

8.2. Obveze voditelja projekta

Opseg poslova voditelja projekta u okviru ove dokumentacije obuhvaća:

- Sudjelovanje u e-Sveučilišta projektnom timu pod vodstvom CARNET-a te timu za provedbu ugovora o javnoj nabavi za implementaciju softverski definiranog mrežnog pristupnog sustava sa sigurnosnom komponentom (Secure SDWAN)
- Koordinaciju svih sudionika iz postupka javne nabave,
- Terminsko i financijsko praćenje i izvještavanje o provedbama aktivnosti,
- Prihvat terenskih kontrola nadležnih, revizorskih i inspekcijskih tijela,
- Koordinaciju aktivnosti i vođenje komunikacije s predstavnikom ustanove vezano za implementaciju aktivne mrežne opreme u ustanovama, te integraciju s postojećom lokalnom računalnom mrežom,
- Organizaciju i provođenje redovitih koordinacija aktivnosti te izradu odgovarajućih zapisnika i izvještaja,
- Kontrola provođenja projektnih aktivnosti te primopredajnih postupaka,
- Izradu potrebnih dnevnih, tjednih i mjesečnih izvješća.

9. Obveze Naručitelja

Obveze Naručitelja u sklopu projekta su:

- Koordinacija aktivnosti,
- Osigurati pristup ustanovama i izvođenje implementacije prema zajednički dogovorenom (od strane odabranog Ponuditelja, Naručitelja i Ustanova) terminskom planu,
- Osiguranje potrebnih konfiguracijskih parametara koji su, ne isključivo:
    - definicija IP adresnog prostora za sve dijelove sustava,
    - osiguranje autentikacije i autorizacije pristupa na središnjem centraliziranom sustavu za – AAI@EduHr.
    - pristup CARNET-ovim sustavima (RT, Netbox i sl.)
- Tijekom radova na lokacijama Naručitelj je dužan osigurati pristup lokaciji Ponuditelju i trajno prisustvo osobe s lokacije kojoj se odabrani Ponuditelj može obratiti sa svim dodatnim pitanjima.