PRILOG 4.

TEHNIČKA SPECIFIKACIJA GRUPA 1 (G1)

Ev. broj: 22-22-VV-OP

**Sadržaj:**

# Opis predmeta nabave

Namjena ovog dokumenta je opisati tehničko rješenje sustava za zaštitu Internet prometa svih škola i njegovih komponenti u sklopu projekta "e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće". Predmet ovog postupka nabave je nabava sigurnosnih, mrežnih i drugih komponenti koje će u cjelini činiti sustav za zaštitu školskih mreža i Internet prometa svih škola. Nabava opisana je kroz nekoliko različitih aktivnosti, koje uključuju:

1. Nabavu sustava za zaštitu Internet prometa svih škola,
2. Nabavu potrebnih pretplata i licenci za tražene funkcionalnosti svih elemenata sustava za zaštitu Internet prometa svih škola
3. Instalaciju i inicijalnu konfiguraciju elemenata sustava za zaštitu Internet prometa svih škola prema zahtjevima Naručitelja,
4. Implementaciju sustava za zaštitu Internet prometa svih škola u postojeću mrežnu infrastrukturu Naručitelja,
5. Edukaciju korisnika.

Odabrani Ponuditelj jamči ispravan rad isporučene opreme i sustava navedenih pod točkom a) tijekom jamstvenog roka. Trajanje i obveze tijekom jamstvenog roka određene su odredbama ove Dokumentacije o nabavi, uključivo prijedlogom ugovora o nabavi koji je sastavni dio Dokumentacije o nabavi te člancima 423.-428. primjenjivog Zakona o obveznim odnosima (NN 35/05, 41/08, 125/11, 78/15, 28/18).

Implementaciju opisanog u predmetu nabave potrebno je isporučiti kao cjelovit projekt kroz uspostavu cjelokupne funkcionalnosti sustava za zaštitu školskih mreža kroz implementaciju i spajanje istog u postojeću mrežnu infrastrukturu Naručitelja, a sve prema zahtjevima Naručitelja opisanim u nastavku dokumenta. Sve aktivnosti obuhvaćene predmetom nabave potrebno je izvršiti pridržavajući se pozitivnih propisa.

# Opis sustava za zaštitu Internet prometa svih škola

Kroz aktivnosti vezane za implementaciju sustava za zaštitu mrežnog prometa svih škola, od ključne je važnosti osigurati nastavnicima i učenicima zaštitu i siguran pristup Internetu kroz CARNET mrežu - **bez narušavanja brzine veze i otežavanja pristupa** svim nastavnim i nenastavnim servisima razvijenim za potrebe škola, te ostatku Interneta.

Detaljan popis traženih funkcionalnosti nalazi se u Prilogu 6. Osnovni zahtjevi za Grupu 1.

## Arhitektura sustava i elementi sustava

Sama arhitektura rješenja i njegovi sastavni elementi te količina istih nisu striktno definirani. Kod arhitekture važno je zadovoljiti se uvijete raspisane u pojedinim poglavljima ovog dokumenta (npr. kapacitivni zahtjevi, visoka dostupnost sustava, spajanje sustava na mrežnu infrastrukturu Naručitelja, skalabilnost … itd.)

## Kapacitivni zahtjevi

Isporučeni sustav za zaštitu mora ispunjavati zahtjeve za mrežnu propusnost, broj istovremenih sesija te broj novih sesija u jedinici vremena zahtijevane od strane Naručitelja.

Tražena minimalna propusnost sustava za zaštitu Internet prometa svih škola je 100 Gbps. Od isporučenog sustava se očekuje da istovremeno može obraditi promet (100 Gbps) prema sljedećim zahtjevima:

* 80 Gbps – minimalna mrežna propusnost sustava s klasičnim usmjeravanjem i inspekcijom paketa na 2 i 3 razini TCP/IP modela (stateful FW) tj. bez uključenih naprednih (sigurnosnih) inspekcija na višim razinama modela,
* 16 Gbps – minimalna mrežna propusnost sustava sa svim uključenim traženim sigurnosnim funkcionalnostima i sustavima napredne zaštite,
* 4 Gbps – minimalna mrežna propusnost sustava s TLS/SSL dekripcijom i sa svim uključenim traženim sigurnosnim funkcionalnostima i sustavima napredne zaštite.

Svi gore navedeni parametri propusnosti se odnose na prosječnu veličinu paketa od 950 Bytea.

Traženi minimalni broj istovremenih sesija koje podržava sustav za zaštitu Internet prometa svih škola je 10.000.000 (slovima: deset milijuna).

Traženi minimalni broj novih sesija po sekundi je 200.000 (slovima: dvjesto tisuća).

## Podrška IPv4 i IPv6

Sve komponente sustava moraju podržavati IPv4 i IPv6 protokole za sve navedene funkcionalnosti sigurnosne zaštite.

## Visoka dostupnost sustava

Sigurnosni sustav za zaštitu mora podržavati konfiguraciju visoke dostupnosti (redundancija komponenti na lokaciji) rada svih logičkih, funkcionalnih i fizičkih komponenti sustava u slučaju kvarova, ispada i prekida rada. Sustav ne smije imati niti jednu točku (SPOF – Single Point of Failure) čiji bi ispad, prekid ili kvar prouzročio bilo što od slijedećeg:

* pad performansi,
* snižavanje propusnosti,
* ispad, prekid ili kvar cijelog sustava,
* ispad, prekid ili kvar pojedine funkcionalnosti sustava.

Također sustav mora biti redundantno spojen na mrežu Naručitelja tako da bude otporan i na ispad pojedine mrežne komponente preko koje je spojen na jezgru CARNET mreže (bilo Naručiteljeve bilo Ponuditeljeve).

## Spajanje komponenti na mrežnu infrastrukturu Naručitelja

Spajanje sustava za zaštitu Internet prometa svih škola u mrežnu infrastrukturu Naručitelja mora biti izvedivo kroz 10G sučelja po 10GBASE-SR standardu i kroz 100G sučelja po 100GBASE-SR4 standardu na način da se korištenjem 10G sučelja može ostvariti propusnost od 80Gb a kroz 100G sučelja maksimalnu propusnost koja je navedena u specifikaciji. Na taj način se želi osigurati mogućnost spajanja sustava u postojeću mrežnu infrastrukturu Naručitelja u trenutku isporuke korištenjem 10G sučelja, ali i mogućnost spajanja s 100G sučelja koja će se koristiti u budućnosti.

Slike prikazuju spajanje u trenutku implementacije ne ukupno potreban broj portova za koji treba uzeti u obzir zahtjev skalabilnosti i visoke dostupnosti.

**

 ***Slika 1.*** *Fizički prikaz spajanja sustava na mrežnu infrastrukturu Naručitelja*



***Slika 2.*** *Logički prikaz spoja sustava na mrežnu infrastrukturu Naručitelja*

P1 i P2 predstavljaju točke u kojima se isporučeni sustav spaja na postojeću mrežnu infrastrukturu Naručitelja. Spoj na infrastrukturu Naručitelja mora biti izveden s minimalno dva fizička uređaja. Na slici prikaza logičkog spoja, slika 2., uređaj N1 je isti uređaj sa oba dvije strane slike no prikazan je dva puta radi logičkog prikaza toka prometa. Isto vrijedi i za uređaj N2. Promet na uređajima N1 i N2 prelazi iz jedne virtualne instance tablice usmjeravanja (vrf) u drugu virtualnu instancu tablice usmjeravanja (vrf) tj globalnu tablicu.

Uređaji za spajanje sustava na mrežnu infrastrukturu Naručitelja može biti izvedeno s dodatnim preklopnicima.

Uređaji sa spajanje sustava na mrežnu infrastrukturu Naručitelja moraju podržavati slijedeće karakteristike za spajanje:

* upravljački protokol za grupiranje fizičkih sučelja 802.3ad (LACP). LACP protokol mora moći grupirati do 8 10G sučelja i do 2 100G sučelja
* 9100 MTU
* 802.1Q (VLAN tagging)
* full-duplex.

Uređaji sa spajanje sustava na mrežnu infrastrukturu Naručitelja moraju imati uključenu tehnologiju za L3/L4 balansiranje/uravnoteženje prometa sa slijedećim značajkama:

* Usmjeravanje prometa na ulaznom sučelju prema L3/L4 značajkama, a neovisno o L2/L3 usmjerivačkim tablicama
* Balansiranje opterećenja temeljeno na težini/vrijednosti čvora
* L4 balansiranje opterećenja temeljeno na virtualnom IP-u
* Balans opterećenja na velikom broju uređaja/poslužitelja
* Podržana visoka dostupnost (eng *failover*) u slučaju ispada čvora
* Funkcionalnost provjere dostupnosti udaljenog IP uređaja putem ICMP proba a u svrhu manipuliranja usmjeravanja prometa
* N + M redundancija (N broj čvorova i M broj hot-standby-eva)
* Automatska reakcija u slučaju kvarova poslužitelja/uređaja
* Usklađena dvosmjernost tokova. Promet iz A–>B i B–>A ide na isti čvor
* Mogućnost preusmjeravanja prometa linearnom brzinom na sve uređaje
* Sposobnost stvaranja klastera uređaja jednog servisa neovisnih o generaciji, modelu ili proizvođaču uređaja
* Ljepljive sesije tj. perzistentne sesije na temelju IP adrese (IP-stickiness)
* VRF podrška,
* Funkcionalnost udruzivanja fizickih linkova na dva razlicita uredaja u jednu logicku vezu (virtual Link Aggregation)
* Podržavati IPv4 i IPv6

Sustav za zaštitu mora omogućiti funkcionalnost propagacije Naručiteljevih ruta koji se može ostvariti na slijedeća dva načina:

* Mod usmjeravanja (”routing” mod)

Naručitelj s isporučenim sustavom podiže dinamički usmjerivački (routing) protokol (OSPFv2, OSPFv3 ili BGP) uz propagaciju minimalno 20.000 ruta

* Transparentni mod
Naručitelj preko isporučenog sustava neovisno o ponuditeljevom sustavu podiže dinamički usmjerivački protokol između svoje opreme.

Ponuditelj prema ponuđenom rješenju mora odrediti tj ponuditi uređaje sa ukupnim brojem sučelja na uređajima koje koristi za spoj na mrežnu infrastrukturu Naručitelja tako da osigurava redundanciju na nivou vatrozida i na nivou cijelog sustava kroz oba navedena standarda 10G i 100G. Ukupan broj sučelja čini broj sučelja kojim se spaja na Naručiteljevu infrastrukturu, sučelja koja se koriste za interna spajanja unutar sustava (ovise o rješenju i naručitelj ne može znati broj) te broj sučelja koji zadovoljavaju uvijete [Skalabilnosti](#_Skalabilnost) i [Visoke dostupnosti](#_Visoka_dostupnost_sustava). Minimalan broj uređaja s kojim se sustav spaja na mrežnu infrastrukturu Naručitelja su dva uređaja.

Ponuđeno rješenje (sustav) za spoj na infrastrukturu Naručitelja mora imati po 8x10Gb + 1x100Gb po svakoj grani (A i B) tj 8x10Gb + 2x100Gb po svakoj grani (A i B) kada se uzme u obzir zahtjev za skalabilnost (potrebno moguće povećanje samo za 100Gb standard).

Ponuditelj mora osigurati sve potrebne primopredajnike i kablove za isporučenu opremu za instalaciju sustava i za spoj na Naručiteljevu mrežnu infrastrukturu.

Međusobno spajanje komponenti unutar sustava za zaštitu može biti izvedeno na bilo koji način koji ispunjava zahtjeve Naručitelja glede skalabilnosti i visoke dostupnosti tj redundancije svake komponente sustava.

Mrežna upravljačka sučelja pojedinih elemenata sustava moraju biti 1G RJ-45. Ako rješenje ima SFP sučelje ponuditelj mora osigurati pravovaljani primopredajnik sa RJ-45 sučeljem.

## Skalabilnost

Idejno rješenje mora biti osmišljeno na način da je moguća proširivost tj skalabilnost sustava tako da se može povećati propusnost i svi ostali kapacitivni parametri dodavanjem novih elemenata u sustav. Sustav se mora moći proširiti dvostruko tj 100% u odnosu na trenutno raspisane kapacitete i propusnosti. Izuzetak skalabilnosti su 10G sučelja koja se koriste sa spoj na mrežnu infrastrukturu Naručitelja za koja nije potrebno osigurati mogućnost dvostrukog proširenja jer će se Naručitelj u tom scenariju oslanjati na 100G sučelja.

## Upravljačka komponenta sustava

Ukoliko Ponuditeljevo rješenje sadrži zasebnu upravljačku komponentu ista može biti isporučena u obliku zasebnog uređaja (eng. *appliance*), u obliku virtualnog poslužitelja ili u obliku kontejnerizirane aplikacije.

U slučaju da Ponuditelj upravljačku komponentu sustava želi isporučiti u obliku virtualnog poslužitelja isti mora podržavati Proxmox hipervizor (KVM/Qemu). U takvoj varijanti ni jedan dio stvarnovremene obrade prometa i primjena sigurnosnih funkcionalnosti se ne smije odrađivati na upravljačkoj komponenti sustava.

## Protokoli za upravljanje i nadzor

Svi elementi u sustavu moraju podržavati slijedeće upravljačko nadzorne protokole:

* SNMPv2, SNMPv3,
* SSHv2,
* Syslog,
* NTP,
* AAA putem RADIUS protokola

## Fizički smještaj sustava

Sustav će se ugrađivati u jedan standardni poslužiteljski ormar. Cijeli sustav koji Ponuditelj isporučuje mora zauzimati maksimalno 22 RU (Rack Unit. 1RU = 1,75“ = 44.45 mm).

## Napajanje uređaja

Napajanja pojedinih komponenti sustava moraju biti 220 V i 50 Hz AC.

Minimalno dva izmjenjiva napajanja po komponenti sustava.

Za potrebe Naručiteljevog planiranja potrošnje električne energije u troškovniku je potrebno navesti snagu pojedine komponente sustava izraženu u vatima (W).

## Pretplate i licence

Sve pretplate (eng. *subscriptions*) i licence potrebne za provedbu traženih funkcionalnosti iz ove Tehničke specifikacije, osnovnih zahtjeva iz Priloga 6. Osnovni zahtjevi za Grupu 1., drugih dokumenata koji su dio ove Dokumentacije te ukoliko je primjenjivo na ponudu dodatnih zahtjeva iz Priloga 8. Dodatni zahtjevi za Grupu 1 moraju biti uključeni u nabavu u trajanju od minimalno 5 (slovima: pet) godina.

# Funkcionalnosti sustava

Od ponuđenog rješenja se očekuje da posjeduje niže navedene sigurnosne i druge funkcionalnosti koje su potrebne za provođenje aktivne zaštite informacijsko komunikacijske opreme, mreža i korisnika na osnovnoškolskim i srednjoškolskim ustanovama, te integraciju sustava s postojećom i planiranom mrežnom infrastrukturom te ostalim nadzornim, upravljačkim i drugim sustavima.

Sve funkcionalnosti koje se odnose na sigurnosne provjere moraju se implementirati u oba smjera toka prometa

Detaljan popis traženih funkcionalnosti nalazi se u Prilogu 6. Osnovni zahtjevi za Grupu 1.

## Zaštita od zlonamjernih datoteka

Radi potrebe sprječavanja preuzimanja zlonamjernog sadržaja s Interneta na uređaje unutar školskih mreža – Ponuditeljevo rješenje mora imati sigurnosne funkcionalnosti koje mogu prepoznati i spriječiti preuzimanje zlonamjernih datoteka. Od sustava za zaštitu se očekuje da u svim široko korištenim nešifriranim protokolima može prepoznati poznate formate datoteka te da nad tim datotekama može provesti određenu analizu u stvarnom vremenu. Sustav mora imati mogućnost prepoznavanja zlonamjernih datoteka na osnovi kriptografskog sažetka, potpisa ili drugih definicija. Uz to, sustav mora pružiti mogućnost primjene iste metode analize nad šifriranim varijantama protokola u slučajevima kad se nad tim istim promotom primjenjuje TLS/SSL dekripcija. Popis traženih funkcionalnosti nalazi se u Prilogu 6. Osnovni zahtjevi G1.

## DNS zaštita

Ponuđeno rješenje mora imati mogućnost provjere DNS prometa te manipulaciju istim. Od sustava za zaštitu Internet prometa svih škola očekuje se da spriječi razlučivanje potencijalno zlonamjernih domena te da postupi prema definiranim akcijama unutar primjene politike/plavila DNS zaštite.

Funkcionalnosti koje se očekuju kod DNS zaštite se odnose isključivo na standardni DNS protokol (53/UDP), a ne i na njegove šifrirane varijante (DNS over HTTPS, DNS over TLS, DNSCrypt).

## IP reputacija

Sustav mora imati mogućnost prepoznavanja i blokiranja potencijalno zlonamjernog prometa sa i prema IP adresama i adresnim prostorima s lošom reputacijom.

To se odnosi poznate izvore zlonamjernih mrežnih aktivnosti kao što su skeniranje, pokušaj iskorištavanja ranjivosti i pokušaj neovlaštenog pristupa te mogućnost prepoznavanja komunikacije s poznatim IP adresama C&C poslužitelja.

## Arhivirane i komprimirane datoteke

Isporučeni sustav mora imati mogućnost provjere sadržaja unutar arhiviranih i komprimiranih datoteka bez dodatne kriptografske zaštite. Formati koji moraju biti podržani su:

* ZIP format,
* RAR format,
* 7Z format,
* gzip format,
* ARJ format,
* CAB format.

Sustav mora imati mogućnost primjene drugih sigurnosnih funkcionalnosti koje se traže ovom dokumentacijom a primjenjive su nad raspakiranim sadržajem arhiviranih i komprimiranih datoteka.

## IPS zaštita

Ponuđeno rješenje mora imati mogućnost otkrivanja i prevencije zlonamjernih mrežnih aktivnosti.

Pravila koje koristi IPS, odnosno IDS, komponenta moraju biti dokumentirana. Pravila uz dodatne opise prijetnji, zahvaćenih uređaja/programa, ozbiljnosti i prirode napada (CVSS), posljedice i pripadajuće CVE oznake.

## TLS/SSL inspekcija

Ponuditeljevo rješenje mora imati mogućnost dekripcije TLS/SSL prometa. Za potrebe dekripcije TLS 1.3 protokola dopuštena je degradacija na isključivo TLS 1.2 protokol.

Sama TLS/SSL inspekcija mora biti izvršena s terminacijom TLS /SSL veza na sigurnosnom sustavu u svrhu provođenja analize nad dekriptiranim/dešifriranim prometom uz uspostavljanje nove TLS/SSL veze između sigurnosnog sustava i krajnjeg uređaja korištenjem svojih certifikata. Prilikom provođenja TLS/SSL inspekcija sustav ne smije forsirati degradiranje TLS/SSL veze između sigurnosnog sustava i poslužitelja za potrebe povećanja performansi rješenja tj degradacija je dopuštena jedino sa TLS 1.3 na TLS 1.2 - sve ostale degradacije potrebno je moći isključiti.

Ponuditeljevo rješenje mora imati mogućnost dekripcije TLS/SSL verzija standardnih komunikacijskih protokola – poglavito HTTP, odnosno HTTPS prometa. Sama funkcionalnost TLS/SSL dekripcije može biti implementirana u istom elementu cjelokupnog sustava kao i sigurnosne funkcionalnosti, ali može biti implementirana u zasebnom uređaju (elementu). Neovisno o varijanti sustava koju Ponuditelj predloži kao rješenje, svi kapacitivni zahtjevi (propusnost, broj sesija, broj novih sesija), zahtjevi visoke dostupnosti te zahtjevi koji se odnose na mogućnost upravljanje putem API-a moraju biti ispunjeni.

Sustav mora omogućavati kreiranje politika za TLS/SSL dekripciju uz mogućnost kreiranja iznimki, to jest izuzimanja određenog dijela prometa iz TLS/SSL dekripcija na temelju izvorišnih i odredišnih IP adresa, odredišnih kategorija i pojedinačnih razlikovnih imena (DN - distinguished name).

Sam sustav mora posjedovati redovno ažurirane i aktualne baza poznatih servisa koji iz tehničkih razloga ne podržavaju TLS/SSL dekripciju.

Detaljan popis traženih funkcionalnosti nalazi se u Prilogu X. Osnovni zahtjevi G1.

## Izuzimanje iz provjere (eng. whitelisting)

Sustav mora imati mogućnost izuzimanja dijelova prometa iz provođenja provjera zbog uštede resursa ili nekog drugog razloga.

Samo izuzimanje prometa iz obrade može biti određeno na temelju IP adresa i/ili adresnih raspona ili na nekom drugom parametru koji jednoznačno opisuje taj promet.

Dio procesa izuzimanja prometa iz provjere (eng. *whitelisting*) je moguće odraditi i na komponentama sustava koje nisu nužno sigurnosne komponente (one komponente koje su sastavni dio isporučenog sustava, ali funkcionalni zadatci im nisu sigurnosne prirode) kako promet generiran od strane nekih pouzdanih servisa ne bi prolazio kroz komponente zadužene za pružanje sigurnosnih funkcionalnosti. Funkcionalnost izuzimanja mora moći jednostavno koristiti bazu poznatih i pouzdanih servisa (kao npr. Microsoft update, Google i sl.) za izuzimanja opisanih u poglavlju „[Baze indikatora i drugih parametara](#_Baze_indikatora_i)“.

## Baze indikatora i drugih parametara

Sustav mora imati redovno ažurirane i aktualne baze koje će se koristiti od strane sigurnosnih funkcionalnosti i drugih funkcionalnosti navedenih u ovome dokumentu. Te baze se odnose na:

* zlonamjerne domene,
* zlonamjerne URL-ove,
* zlonamjerne IP adrese i adresne raspone,
* potpise i/ili kriptografske sažetke zlonamjernih datoteka,
* IPS/IDS potpisa/pravila,
* baze poznatih servisa koji iz tehničkih razloga ne podržavaju TLS/SSL dekripciju.

Uz to sustav mora posjedovati aktualnu i redovno ažuriranu bazu poznatih servisa za potrebu izuzimanja (eng. *whitelisting*) istih iz inspekcije. Identificirani servisi moraju imati visok stupanj razlučivosti, to jest unutar jednog davatelja usluga mora moći identificirati različite usluge/servise.

## Dnevnički zapisi (sistemsko logiranje)

Za potrebe integracija s zasebnim SIEM rješenjem te vanjskim poslužiteljem za dnevničke zapise (syslog server) sve funkcionalne komponente ponuđenog rješenja moraju imati mogućnost slanja dnevničkih zapisa u syslog formatu na udaljene sustave uz zadržavanje lokalnih dnevničkih zapisa.

## API podrška

Za potrebe razvoja vanjskih portala za korisnike nužno je da sustav za upravljanje i nadzor mreže podržava rad s API upitima. Detaljan popis traženih funkcionalnosti se nalazi u Prilogu 6. – Osnovni zahtjevi G1.

Za sve API pozive Ponuditelj je obvezan osigurati sljedeće zahtjeve:

* Sa svih komponenti sustava moguć je transfer podataka (dohvaćanje i slanje podataka) korištenjem REST API-a. Transfer podataka kroz API se mora obavljati korištenjem HTTPS-a. Očekivani formati podataka su: XML ili JSON. Ovaj uvjet se odnosi na sve API zahtjeve.
* Sve komponente sustava za zaštitu Internet prometa svih škola podržavaju upravljanje i konfiguriranje putem REST API-a za sljedeće:
	+ kreiranje i upravljanje mrežnih objekata (IP adrese, IP adresni rasponi te skupovi i kombinacije istih),
	+ kreiranje pravila za izuzimanje (eng. *whitelisting*) i upravljanje istima,
	+ kreiranje pravila vatrozida i upravljanje istim pravilima,
	+ kreiranje sigurnosnih profila i upravljanje istima,
* Navedeni zahtjevi za pojedinu API funkcionalnost mogu biti zadovoljeni većim brojem API poziva.
* Svi API pozivi kojima se zadovoljavaju Osnovni zahtjevi tehničke specifikacije moraju biti implementirani u sklopu programskog rješenja proizvođača opreme, a bez korištenja alata koji nisu razvijeni od strane proizvođača.

## Analiza u izoliranom okruženju (eng. Sandbox)

Sustav analize u izoliranom okruženju mora omogućiti analizu 1.000 jedinstvenih datoteka u satu u vršnom opterećenju a 11.000 u danu. Naručitelj preferira analizu na lokaciji instalacije rješenja (on-premise) no prihvaća i drugi oblik izvedbe ove funkcionalnosti tj rješenje u oblaku (cloud). Rješenje u oblaku mora datoteke obrađivati unutar EU-a tj ne smije datoteke slati izvan granica EU-a. Također ako se analiza radi u oblaku ponuditelj mora osigurati dokument o upravljanju privatnim podatcima (eng *Product Privacy Data Sheets*) koja se odnosi na uslugu analize u oblaku.

## Izvještavanje

Ponuditeljevo rješenje mora imati mogućnost izvještavanja na više načina:

* statistički prikaz detektiranih zlonamjernih pojava zadanoj štićenoj IP adresi/domeni ili rasponu IP adresa,
* statistički prikaz svih detektiranih zlonamjernih pojava po broju detektiranih/blokiranih,
* statistički prikaz jedne zadane detektirane zlonamjerne pojave po broju ukupno detektiranih/blokiranih,
* statistički prikaz gore opisanog prema zadanom vremenskom razdoblju,
* mora podržavati isporuku izvještaja u jednom od slijedećih formata: PDF, HTML, CSV, DOC, DOCX.

# Jamstvo

Odabrani Ponuditelj izdaje jamstvo za ispravnost opreme i cjelokupnog sustava u razdoblju od minimalno 60 mjeseci od dana potpisivanja primopredajnog zapisnika za implementaciju sustava za zaštitu Internet prometa svih škola.

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 i da je kompatibilna s ostatkom isporučenog sustava. Zamjenu pojedine komponente isporučenog sustava odabrani Ponuditelj će izvršiti u roku od 14 radnih 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 slično.

Odabrani Ponuditelj je dužan predati Naručitelju jamstva za ispravnost opreme, točnije jamstvene listove izdane od strane proizvođača opreme u trajanju kako je navedeno gore 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.

Tehnička podrška

Ponuditelj je obvezan, prilikom potpisivanja ugovora ili najkasnije prilikom isporuke opreme, Naručitelju dostaviti kontakt podatke centra za tehničku podršku za prijavu problema, kvara ili drugog nedostatka na isporučenoj opremi, kroz cijelo razdoblje trajanja jamstvenoga roka. Svi oblici podrške moraju biti dostupni na hrvatskom jeziku.

Ponuditelj obavezan je pružiti Naručitelju sljedeće usluge tehničke podrške:

* Osigurati prijem prijave problema, kvara ili drugog nedostatka putem: telefona, elektronske pošte ili web stranice sustava za prijavu problema,
* Osigurati rješavanje problema putem: telefona, elektronske pošte ili web stranice sustava za prijavu problema,
* Prema potrebi osigurati rješavanje problema i putem izlaska ovlaštenog tehničara na lokaciju Naručitelja,
* Ukoliko problem, kvar ili drugi nedostatak nije u mogućnosti otkloniti na lokaciji Naručitelja, Ponuditelj će opremu o svome trošku odvesti u ovlašteni servis i popravljeno vratiti iz servisa na lokaciju Naručitelja.

Tehnička podrška Ponuditelj za vrijeme jamstvenog roka mora omogućiti prijavu problema i kvarova svakim danima od **8:00 – 16:00 s najdužim odzivom od jednog ranog dana od trenutka prijave** te je dužan u tom periodu započeti s analizom i rješavanjem problema. Ako problem nije moguće ukloniti u roku od **pet** **dana** od trenutka prijave problema tada je Ponuditelj dužan isporučiti Naručitelju novu opremu u roku ne dužem od definiranog vremena potrebnog za zamjenu neispravne opreme.

Ukoliko se problem može otkloniti udaljenim pristupom (u roku od **pet dana**) tada nije obavezno da djelatnik Ponuditelja izlazi na lokaciju, ali kvar mora biti otklonjen u roku ne dužem od definiranog vremena potrebnog za zamjenu neispravne opreme.

Ponuditelj za vrijeme trajanja jamstva mora Naručitelju omogućiti preuzimanja aktualnih verzija softvera isporučene opreme obuhvaćene ovim postupkom Nabave s ciljem otklanjanja nedostataka u funkcioniranju opreme i sustava te sigurnosnih ranjivosti.

# Edukacija korisnika

Odabrani Ponuditelj dužan je osigurati edukaciju o svim komponentama isporučenog sustava te o svim njihovim funkcionalnostima koje su tražene u ovoj nabavi ili se koriste za izvedbu isporučenog sustava, a bez dodatnog troška po Naručitelja.

Ciljane skupine polaznika edukacije su djelatnici i suradnici Naručitelja.

Sve edukacije se moraju provesti uživo u obliku radionica na hrvatskom jeziku.

Kroz radionice polaznici moraju proći kroz praktične primjere i zadatke konfiguracija na ekvivalentnom sustavu kao i sustavu koji je predmet ove nabave (*hands-on i demo*).

Potrebno je održati dvije radionice. Mjesto za održavanje edukacije je dužan osigurati Ponuditelj osim ako Naručitelj ponudi svoje prostore. Vrijeme edukacije bit će određeno u dogovoru s Naručiteljem tijekom provedbe ugovora.

Maksimalni broj polaznika po radionici 5 osoba. Minimalno ukupno trajanje radionice je 40 sati kroz 5 radna dana.

U slučaju više sile, uz odobrenje Naručitelja, edukacije se mogu iznimno odgoditi.

# 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 isporučenog sustava definirat će se u suradnji s Naručiteljem nakon potpisivanja ugovora.

Ponuditelj je dužan prije isporuke opreme Naručitelju dostaviti konfiguracijske primjere za pojedine funkcionalnosti navedene u tehničkoj specifikaciji te tehničku podršku prilikom implementacije istih.

Ponuditelj mora osigurati da sav instalirani softvere uređaja bude na zadnjoj stabilnoj verziji, a koja je preporučena od strane proizvođača opreme.

# Tehničko-funkcionalne specifikacije predmeta nabave

Tablice tehničko-funkcionalnih zahtjeva navedene u Prilogu 6. – Osnovni zahtjevi za Grupu 1 moraju sadržavati DA/NE odgovore na opis tehničke karakteristike, te ih je ispunjene odabrani Ponuditelj obvezan priložiti u ponudi.

Obveza je odabranog Ponuditelja izrijekom navesti točnu specifikaciju (proizvođač, model) te priložiti tehničku dokumentaciju proizvođača ponuđenog rješenja i navesti broj stranice tehničke dokumentacije na kojoj se nalazi opis svake komponente sustava koja se nalazi u ponudi, a kojom se zadovoljavaju pojedini tehničko-funkcionalni zahtjevi.

Odabrani Ponuditelj u ponudi mora dostaviti TEHNIČKU DOKUMENTACIJU PROIZVOĐAČA I/ILI POTVRDU PROIZVOĐAČA, jednakovrijedan dokument ili izjavu odabranog Ponuditelja kojom dokazuje da su TEHNIČKO FUNKCIONALNE KARAKTERISTIKE ponuđenog proizvoda u skladu s karakteristikama traženim u Prilogu 6. – Osnovni zahtjevi Dokumentacije o nabavi. Naručitelj zadržava pravo da provjeri ispravnost navoda na službenim Web stranicama proizvođača.

Sve navedene i tražene funkcionalnosti u ovoj dokumentu i pripadajućim dokumentima sustav za zaštitu mora biti isporučen sa svim potrebnim i pripadajućim komponentama te licencama tako da su opisane i tražene funkcionalnosti ostvarive u trenutku isporuke opreme bez dodatnih troškova za Naručitelja. Kako je navedeno u Prilogu 6. – Osnovni zahtjevi za Grupu 1 potrebno je ponuditi i ispuniti tablice i priložiti dokaze za sljedeću opremu:

* Sustav za zaštitu Internet prometa svih škola

Ukoliko je primjenjivo na ponudu, potrebno je ponuditi i ispuniti tablice i priložiti dokaze za dodatne zahtjeve Prilog 8. – Dodatni zahtjevi za Grupu 1 za sljedeću opremu:

* Sustav za zaštitu Internet prometa svih škola

# Obveze odabranog Ponuditelja

U sklopu projekta obveze odabranog Ponuditelja su:

* Izrada plana aktivnosti za implementaciju sustava za zaštitu Internet prometa svih škola. Izrada vremenskog plana svih aktivnosti. Vremenski plan je potrebno usuglasiti sa Naručiteljem,
* Sudjelovanje na redovitim koordinacijama sukladno dogovoru s Naručiteljem,
* Vođenje projekta,
* Izvještava o napretku projekta implementacije svaka dva tjedna,
* Isporuka opreme na lokacije Naručitelja navedene u Dokumentaciji o nabavi ili drugu lokaciju u dogovoru s Naručiteljem,
* Implementacija elemenata sustava za zaštitu Internet prometa svih škola po pravilima struke i pozitivnih propisa,
* Instalacija i konfiguracija elemenata sustava za zaštitu Internet prometa svih škola iz ovog projekta od strane ovlaštenih i stručnih osoba odabranog Ponuditelja u skladu sa zahtjevima Naručitelja,
* Testiranje osnovnih funkcionalnosti i sigurnosnih funkcionalnosti sustava prilikom prespajanja pojedinog bloka škola u dogovoru s Naručiteljem (postavljanje u produkcijsku okolinu),
* isporučiti dokumentirano izvedbeno stanje implementacije rješenja i rezultate testiranja iz prethodne alineje
* Isporučiti plan i sadržaj edukacije,
* Edukacija korisnika kroz dvije radionice,
* Isporučiti uputstva za upotrebu i konfiguriranje te edukativne materijale za uređaje isporučene u sustavu u elektroničkom obliku s posebnim naglaskom na funkcionalnosti navedene u ovom dokumentu,
* Postavljanje oznaka vidljivosti EU sufinanciranja na svim fizičkim isporučenim komponentama
* Komunicira s razvojnim timom proizvođača vezano za razvoj, testiranje i implementaciju traženih API funkcionalnosti,
* Isporučiti razrađene i dokumentirane procedure za nadogradnju sustava,
* Isporučiti izrađeno tipično tehničko rješenje dekripcije prometa škola po tipovima škola,
* Podrška Naručitelju u realizaciji zacrtanih ciljeva i potreba.

# Obveze Naručitelja

Obveze Naručitelja u sklopu projekta su:

* Koordinacija aktivnosti,
* Osigurati pristup do mjesta izvršenja ugovora,
* Osigurati potrebne tehničke resurse za integraciju sustava za zaštitu Internet prometa svih škola s postojećom mrežnom infrastrukturom,
* Osiguranje potrebnih konfiguracijskih parametara.