PRILOG 5.

TEHNIČKA SPECIFIKACIJA
GRUPA 2 (G2)

Ev. broj: 22-22-VV-OP

**Sadržaj:**

[1. Opis predmeta nabave 4](#_Toc97647302)

[2. Opis sustava za zaštitu prometa elektroničke pošte 5](#_Toc97647303)

[Arhitektura sustava 5](#_Toc97647304)

[Kapacitivni zahtjevi 6](#_Toc97647305)

[Podrška IPv4 i Ipv6 7](#_Toc97647306)

[Visoka dostupnost sustava 7](#_Toc97647307)

[Spajanje komponenti na mrežnu infrastrukturu Naručitelja 7](#_Toc97647308)

[Skalabilnost 8](#_Toc97647309)

[Upravljačka komponenta sustava 9](#_Toc97647310)

[Napajanje uređaja 9](#_Toc97647311)

[Protokoli za upravljanje i nadzor 9](#_Toc97647312)

[Pretplate i licence 10](#_Toc97647313)

[3. Funkcionalnosti sustava 10](#_Toc97647314)

[Detekcija i blokiranje poruka elektroničke pošte 10](#_Toc97647315)

[Detekcija i blokiranje masovne kampanje 11](#_Toc97647316)

[Spremanje zlonamjernih poruka u karantenu 11](#_Toc97647317)

[Obavještavanja 11](#_Toc97647318)

[Blokiranje neželjene pošte 12](#_Toc97647319)

[Dnevnički zapisi (sistemsko logiranje) 12](#_Toc97647320)

[API podrška 12](#_Toc97647321)

[Analiza u izoliranom okruženju (eng. Sandbox) 13](#_Toc97647322)

[Izvještavanje 13](#_Toc97647323)

[4. Jamstvo 14](#_Toc97647324)

[5. Edukacija korisnika 16](#_Toc97647325)

[6. Usluge instalacije i konfiguracije 17](#_Toc97647326)

[7. Tehničko-funkcionalne specifikacije predmeta nabave 18](#_Toc97647327)

[8. Obveze odabranog Ponuditelja 19](#_Toc97647328)

[9. Obveze Naručitelja 20](#_Toc97647329)

# Opis predmeta nabave

Namjena ovog dokumenta je opisati tehničko rješenje sustava za zaštitu prometa elektroničke pošte 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 sustava za zaštitu prometa elektroničke pošte i sandučića elektroničke pošte na školama. Nabava opisana je kroz nekoliko različitih aktivnosti, koje uključuju:

1. Nabavu sustava za zaštitu prometa elektroničke pošte,
2. Nabavu potrebnih pretplata i licenci za tražene funkcionalnosti svih elemenata sustava za zaštitu prometa elektroničke pošte,
3. Instalaciju i inicijalnu konfiguraciju elemenata sustava za zaštitu prometa elektroničke pošte,
4. Integraciju sustava za zaštitu prometa elektroničke pošte u postojeći sustav 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).

Implementacija projekta uključuje isporuku i uspostavu cjelovite funkcionalnosti koju čine elementi sustava za zaštitu prometa elektroničke pošte te povezivanje opreme na postojeće računalne sustave i mrežnu infrastrukturu Naručitelja.

Implementaciju opisanog u predmetu nabave potrebno je isporučiti kao cjelovit projekt kroz uspostavu cjelokupne funkcionalnosti sustava za zaštitu prometa elektroničke pošte kroz implementaciju i spajanje istog u postojeće računalne sustave i 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 prometa elektroničke pošte

Kroz aktivnosti vezane za implementaciju sustava za zaštitu prometa elektroničke pošte je cilj zaštititi sandučiće elektroničke pošte na školama.

Detaljan popis traženih funkcionalnosti nalazi se u Prilogu 7. Osnovni zahtjevi za Grupu 2.

## Arhitektura sustava

Kod postojećeg sustava elektroničke pošte MX zapis za štićenih sandučića (“@skole.hr”) se nalazi na javnoj adresi uravnoteživača prometa (eng. *load balancer)* koji poruke elektroničke pošte usmjerava na jednog od dva interna mail poslužiteljima. Ta dva interna *mail* poslužitelja (MX 1 i MX 2 na Slici 1.) imaju funkcionalnost filtriranja spam poruke te zadatak usmjeravanja poruka elektroničke pošte prema korisnikovom sandučiću elektroničke pošte koji se može nalaziti na tri različite lokacije: lokalnom mail serveru ili na jednom od dvoje ponuđenih davatelja usluge u oblaku. Na Slici 1. je prikazan trenutačni sustav elektroničke pošte.



***Slika 1.*** Trenutačno stanje sustava elektroničke pošte – logički prikaz

Željeno stanje nakon implementacije je da dva MTA agenta (*Mail Transfer Agent*) MX1 i MX2 prema određenoj logici naručitelja prosljeđuju dio poruka na sustav zaštite elektroničke poruke. Sustav zaštite treba sve proslijeđene poruke od MX1 i MX2 prihvatiti i procesirati tj nad njima izvršiti sigurnosne provjere i funkcionalnosti tražene u ovom dokumentu i drugim dokumentima vezanih za ovaj predmet nabave. Sustav zaštite elektroničke pošte nakon izvršenih sigurnosnih provjera mora moći proslijediti poruke prema odredišnim sandučićima ili vratiti prema MX1 ili MX2 ovisno o izboru implementacije naručitelja. Sustav zaštite bez licenci (nakon njihovog isteka) mora moći raditi osnovno usmjeravanje elektroničkih poruka.

Na Slici 2. je prikazano željeno stanje sustava elektroničke pošte koji će uključivati komponente za zaštitu prometa elektroničke pošte.



***Slika 2.*** Željeno stanje sustava elektroničke pošte – logički prikaz

## Kapacitivni zahtjevi

Isporučeni sustav za zaštitu mora ispunjavati zahtjeve za propusnost određene količine poruka elektroničke pošte u sekundi i broj korisničkih računa odnosno sandučića elektroničke pošte zahtijevane od strane Naručitelja.

Maksimalan broj sandučića iznosi 520.000.

Tražena količina poruka elektroničke pošte koju sustav za zaštitu mora zadovoljiti iznosi 75.800 poruka u satu u najopterećenijim vremenskim periodima.

Razdioba veličine mailova je prema slijedećoj tablici:

|  |  |
| --- | --- |
| **Veličina u KB** | **broj poruka u jednom satu**  |
| **0-99** | 67.000 |
| **100-999** | 8.000 |
| **1000-9999** | 600 |
| **10.000- i više** | 200 |

## 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 rada svih logičkih, funkcionalnih i fizičkih komponenti sustava u slučaju kvara, ispada ili prekida rada na način da se osigura neometani protok mailova bez većeg kašnjenja. Sustav ne smije imati niti jednu točku čiji bi ispad, prekid ili kvar prouzročio ispad, prekid ili kvar cijelog sustava ili pojedine funkcionalnosti sustava (SPOF – Single Point of Failure).

Također sustav mora biti redundantno spojen na mrežu tako da bude otporan i na ispad jedne mrežne komponente preko koje je spojen na jezgru CARNET mreže,

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 prometa elektroničke pošte svih škola na mrežnu infrastrukturu Naručitelja mora biti izvedivo kroz 10G sučelja po 10GBASE-SR standardu.



***Slika 3.*** *-*  *Fizički prikaz spajanja sustava na mrežnu infrastrukturu Naručitelja*

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 rješenja za zaštitu elektroničke pošte i na nivou cijelog sustava (npr. cijeli sustav mogu sačinjavati mrežne komponente i uređaji za zaštitu elektroničke pošte). 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.

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

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 se omogućava skalabilnost. To jest, mogućnost povećana propusnosti poruka elektroničke pošte i svi ostali kapcitivni parametari dodavanjem novih elemenata u sustav. Sustav se mora moći proširiti dvostruko tj 100% u odnosu na trenutno raspisane kapacitete i propusnosti.

## 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 isporučuje u obliku virtualnog poslužitelja koja podržava OpenStack tj. KVM bazirani hipervizor isti može biti udomljen na infrastrukturi kojom raspolaže Naručitelj. Prihvatljiva je isporuka upravljačke komponentu koja ne podržava OpenStack/KVM kada je ista isporučena i pokrenuta na zasebnom uređaju s podržanim hipervizorom, tada u ponudu trebaju biti uključeni svi troškovi dodatnih licenci i hardvera sustava upravljačke komponente, podrška za uključeni dodatni sustav tijekom perioda održavanja i dodatni sustav pokriven jamstvenim periodom.

## Napajanje uređaja

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

Minimalno dva izmjenjiva napajanja po komponenti sustava.

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

## Protokoli za upravljanje i nadzor

Svi elementi u sustavu moraju podržavati slijedeće upravljačko nadzorne protokole:

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

## Pretplate i licence

Sve pretplate (eng. *subscriptions*) i licence potrebne za provedbu traženih funkcionalnosti iz ove Tehničke specifikacije, osnovnih zahtjeva iz *Priloga 7. Osnovni zahtjevi za Grupu 2.*, drugih dokumenata koji su dio ove Dokumentacije te ukoliko je primjenjivo na ponudu dodatnih zahtjeva iz *Priloga 9. Dodatni zahtjevi za Grupu 2* moraju biti uključeni u nabavu u trajanju od 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 prometa elektroničke pošte i sandučića elektroničke pošte korisnika na osnovnoškolskim i srednjoškolskim ustanovama, te integraciju sustava s postojećim i planiranim računalnom sustavima i mrežnom infrastrukturom te ostalim nadzornim, upravljačkim i drugim sustavima.

Sustav mora moći sve sigurnosne funkcionalnosti obavljati u oba smjera protoka poruka.

## Detekcija i blokiranje poruka elektroničke pošte

Ponuditeljevo rješenje mora imati metode i tehnike za detekciju i blokiranje poruka elektroničke pošte prema:

1. malicioznom privitku,

Svaku poruku koja je usmjerena prema sigurnosnom uređaju mora proći kroz provjeru da li sadrži privitak i ako sadrži da li se radi o malicioznom privitku. Poruke koje se označe kao sigurne isporučuju se prema krajnjem korisniku, a poruke za koje se ne može utvrditi radi li se o zlonamjernoj ili legitimnoj prelaze na sljedeći nivo sigurnosne provjere ili se automatski šalju u karantenu.

1. tipu privitka,

Sustav mora imati mogućnost provjere tipa privitka te na osnovu tog podatka odlučiti šalje li se taj privitak u karantenu ako se radi o izvršnim datotekama (npr. .exe, .dll, .sh, itd.) ili se nastavlja daljnji tijek provjere.

1. malicioznoj poveznici,

Sustav mora detektirati svaku poveznicu unutar tijela poruke, te imati način provjere što se iza takve poveznice nalazi (mogućnost otvaranja poveznice u zaštićenoj okolini ili provjera na nekim od javnih servisa, npr. Virustotal). Sustav mora detektirati maliciozne poveznice u tijelu poruke koje su skraćene.

1. Reputaciji i kategorizaciji poveznice,

Sustav mora detektirati vrste elektroničke poruke analizirajući kategorizaciju i reputaciju poveznica/URL-a unutar tijela elektroničke poruke

1. ključnim riječima.

Sustav mora imati mogućnost filtriranja poruka prema sadržaju naslova ili tijela, tj. slanja poruka u karantenu ako sadrže neke nedozvoljene riječi koje su definirane od strane korisnika sigurnosnog sustava

Svaku poruku za koju se utvrdi da sadrži privitak koji je na inicijalnoj provjeri označen kao "opasan" sustav mora poslati na dubinsku analizu privitka kako bi se sa stopostotnom sigurnošću utvrdili radi li se o malicioznom privitku i koji je stupanj opasnosti za korisnika.

Ukoliko je primjenjivo na ponudu, uređaj može imati mogućnost slanja privitka na izoliranu okolinu na dodatnu analizu datoteke (eng. *sandbox*). Kao što je navedeno u *Prilogu 9*. ove Dokumentacije.

Uz gore navedene načine detekcije poruka elektroničke pošte sustav mora imati mogućnost prepoznavanja zlonamjernih datoteka na osnovi kriptografskog sažetka, potpisa ili drugih definicija.

## Detekcija i blokiranje masovne kampanje

Kada jedna te ista poruka (ili vrlo slična poruka – npr sa 80% istog teksta) bude poslana na veliki broj adresa sustav mora prepoznati da se radi o masovnoj kampanju usmjerenoj prema korisnicima te istu zaustaviti odnosno blokirati.

## Spremanje zlonamjernih poruka u karantenu

Radi mogućnosti lažne detekcije svaka poruka za koju sustav nekom od metoda sigurnosne provjere ustanovi da je zlonamjerna sustav mora istu pohraniti u karantenu na određeni vremenski period koji se može korisnički prilagoditi. Ponuditelj mora osigurati dostatan prostor za pohranu poruka u karanteni za minimalni vremenski period od 3 mjeseca.

Za svaku poruku elektroničke pošte pohranjenu u karanteni sustav mora imati osiguran način propuštanja iste iz karantene ili trajnog brisanja u bilo kojem trenutku.

Funkcionalnost jedinstvene karantene tj centralnog pristupa karanteni na razini cijelog sustava je poželjna i kao takva će se dodatno bodovati kroz dodatne zahtjeve.

## Obavještavanja

Kada sigurnosni sustav označi poruku elektroničke pošte zlonamjernom i pohrani ju u karantenu potrebno je osigurati mogućnost slanja obavijesti administratoru sustava o zlonamjernim aktivnostima kao i slanja obavijesti primatelju poruke kome je ista upućena.

## Blokiranje neželjene pošte

Sustav mora imati razvijen način detekcije i blokiranja neželjenih poruka, masovnih reklamnih poruka.

## 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 poželjno je da sustav za upravljanje podržava rad s API upitima koje nije nužno no dodatno će se bodovati.

Za sve API pozive da bi Ponuditelj dobio dodatne bodove obvezan je 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 školskih mreža podržavaju upravljanje i konfiguriranje putem REST API-a za sljedeće:
	+ dodavanje pravila na crnu listu i listu izuzimanja („black and white lists“),
	+ otpuštanje poruka elektroničke pošte iz karantene,
	+ dohvaćanje popisa poruka koje su u karanteni, dohvaćanje svih poruka i dohvaćanje popisa poruka prema zadanom primatelju/pošiljatelju,
* 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 mrežne 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 privitka tj 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 privitke i datoteke obrađivati unutar EU-a tj ne smije privitke i 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:

* prikaz statistike o ukupnom broju obrađenih poruka elekt. pošte,
* prikaz statistike prema načinu detekcije (maliciozna poveznica/privitak itd.),
* prikaz statistike prema pošiljatelju i primatelju elekt. pošte po broju poslanih i primljenih poruka elekt. pošte
* prikaz statistike top poruka elekt. pošte prema izvorišnom/destinacijskom poslužitelju
* statistički prikaz gore opisanog prema zadanom vremenskom razdoblju,
* mora podržavati isporuku izvještaja u jednom od slijedećih formata: PDF,HTML,CSV,DOC,DOCX formatu

# Jamstvo

Odabrani Ponuditelj izdaje jamstvoza 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 **0:00 – 24:00 s najdužim odzivom od 8h 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 7. – Osnovni zahtjevi za Grupu 2 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 7. – 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 7. – Osnovni zahtjevi za Grupu 2 potrebno je ponuditi i ispuniti tablice i priložiti dokaze za sljedeću opremu:

* Sustav za zaištu prometa elektroničke pošte

Ukoliko je primjenjivo na ponudu, potrebno je ponuditi i ispuniti tablice i priložiti dokaze za dodatne zahtjeve Prilog 9. – Dodatni zahtjevi za Grupu 2 za sljedeću opremu:

* Sustav za zaštitu prometa elektroničke pošte

# Obveze odabranog Ponuditelja

U sklopu projekta obveze odabranog Ponuditelja su:

* Izrada vremenskog plana aktivnosti za implementaciju sustava za zaštitu prometa elektroničke pošte. . 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 prometa elektroničke pošte po pravilima struke i pozitivnih propisa,
* Instalacija i konfiguracija elemenata sustava za zaštitu prometa elektroničke pošte iz ovog projekta od strane ovlaštenih i stručnih osoba odabranog Ponuditelja u skladu sa zahtjevima Naručitelja,
* Testiranje osnovnih funkcionalnosti i sigurnosnih funkcionalnosti sustava integracije sustava za zaštitu u postojeći sustav elektroničke pošte 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 isporučen sustav i uređaje 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,
* 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 prometa elektroničke pošte u postojeći sustav elektroničke pošte,
* Osiguranje potrebnih konfiguracijskih parametara.