

Projektna naloga in ponudbeni predračun
Nakup, vzpostavitev in vzdrževanje požarne
pregrade podatkovnega centra

(int. ev. št. 000131/2026)

DARS

Vsebina

1.	Predmet naročila.....	3
2.	Tehnična specifikacija	3
2.1	Obstoječa rešitev.....	3
2.2	Končno stanje.....	4
2.3	Tehnične in funkcionalne zahteve opreme sistema požarne pregrade	4
2.3.1.	Splošne zahteve glede strojne in programske opreme požarne pregrade:	4
2.3.2.	Zahtevane zmogljivosti strojne opreme požarne pregrade podatkovnega centra .	4
2.3.3.	Tehnične zahteve požarne pregrade za strojno opremo:.....	5
2.3.4.	Funkcionalne zahteve požarne pregrade:	5
2.3.5.	Tehnične zahteve za centralni upravljalni sistem požarnih pregrad	6
2.4	Zahteve za garancijo proizvajalca za strojno in programsko opremo	7
2.5	Storitve implementacije	7
2.6	Storitve vzdrževanja	8
2.6.1.	Lokacije naročnika	10
2.6.2.	Povezljivost lokacij	10
2.7	Specifikacija zahtevane dokumentacije	10
2.7.1.	Izvedbeni načrt	10
2.8	Visokonivojska tehnična dokumentacija	11
2.8.1.	Nizkonivojska tehnična dokumentacija	11
2.8.2.	Dokumentacija postopkov uvedbe, testiranja in upravljanje rešitve.....	11
2.8.3.	Izobraževanje.....	12
3.	Izvedba pogodbenih obveznosti	12
3.1	Redno obratovanje.....	12
4.	Ponudbeni predračun.....	13

1. Predmet naročila

Predmet javnega naročila je nakup sistema požarnih pregrad za zaščito podatkovnega centra poslovnega omrežja DARS. Javno naročilo obsega dobavo opreme, podporo proizvajalca za obdobje 5 let ter izvedbo storitev implementacije in vzdrževanja za obdobje 5 let:

- Nakup požarne pregrade v HA načinu s pripadajočimi licencami (strojna in programska oprema):
- Storitve implementacije:
 - namestitev in konfiguracija opreme v okolju naročnika,
 - integracija in optimizacija opreme,
 - testiranje delovanja,
 - selitev produkcijskih podatkovnih omrežij,
 - izdelava dokumentacije in prenos znanja,
- Vzdrževanje in podpora proizvajalca (B2B support) za obdobje 5 let:
 - garancija strojne in programske opreme za čas pogodbe,
 - pravice do posodabljanja programske opreme ter varnostnih podpisov vključenih v naročnino v času trajanja pogodbe
- Storitve vzdrževanja (mesečni pavšal) za obdobje 5 let:
 - tehnična podpora in servisna popravila s strani partnerja za strojno in programsko opremo.

Oprema je namenjena varovanju dostopa do/med omrežji podatkovnega centra in omejitvi uporabnikov pri dostopu do slednjih. Zahtevana je postavitve v visoki razpoložljivosti. Požarna pregrada mora nuditi varnostne mehanizme »naslednje generacije«. Oprema bo nameščena v dveh geografsko ločenih podatkovnih centrih, kjer povprečne zakasnitve prenosne poti ne presegajo 20 ms.

Cilj javnega naročila je povišanje varnosti v podatkovnem centru z uvedbo dodatne segmentacije omrežij, kontrole komunikacije med omrežji z možnostjo uporabe aplikacijskih pravil ter zaščite proti vdorom (IPS) podatkovnega centra.

2. Tehnična specifikacija

2.1 Obstoječa rešitev

Naročnik ima v svojem okolju trenutno robno požarno pregrado, ki se uporablja tudi za omrežja, namenjena zaščiti podatkovnega centra.

Določen del podatkovnih omrežij se trenutno ščiti s pomočjo robne požarne pregrade, večina omrežij pa se zaključuje na L3 stikalih brez dodatnih omejitev.

2.2 Končno stanje

Cilj uvedbe požarne pregrade podatkovnega centra je preselitev notranjih omrežij z robne požarne pregrade ter omrežij, ki se zaključujejo na L3 nivojskih stikalih, na fizično ločeno požarno pregrado. S tem se zagotovi konsolidacija in jasna ločitev med robnimi in podatkovnimi omrežji.

Vzpostavljena bo nadzorovana komunikacija med podatkovnimi omrežji, hkrati pa bo zagotovljena ločitev uporabniških segmentov od neposrednega dostopa do teh omrežij, kar bo povečalo raven varnosti dostopa.

Požarna pregrada podatkovnega centra bo dodatno omogočala aplikacijsko ločevanje prometnih tokov ter zagotavljala zaščito strežnikov z mehanizmom za preprečevanje vdorov (IPS).

2.3 Tehnične in funkcionalne zahteve opreme sistema požarne pregrade

2.3.1. Splošne zahteve glede strojne in programske opreme požarne pregrade:

- Rešitev zahteva dva člana gruče požarnih pregrad.
- Rešitev mora omogočati visoko razpoložljivost v načinu aktivni-aktivni ali aktivni-pasivni. Izvajalna modula morata biti ločena od upravljalnega modula.
- Podpora delovanja v načinu gruče znotraj istega ter geografsko ločenega podatkovnega centra.
- Ponujen proizvajalec požarne pregrade mora imeti v svojem portfelju podprto implementacijo virtualizirane požarne pregrade v oblaknih ponudnikih (kot npr. Microsoft Azure ali Amazon Web Services (AWS)).
- Rešitev ne sme biti omejena na število končnih uporabnikov ter strežnikov, ki prehajajo varnostne komponente.
- Prisotnost v »Forrester Wave« kvadrantu vodilnih proizvajalcev požarnih pregrad vsaj v letu 2024 ali 2025.

2.3.2. Zahtevane zmogljivosti strojne opreme požarne pregrade podatkovnega centra

Minimalne strojne zmogljivosti požarne pregrade v načinu visoke razpoložljivosti (za vsak posamezen član gruče):

- Prepustnost požarne pregrade vsaj **45 Gbps** (tip prometa: Lab test performance – velikost paketa UDP 1024B).
- Zaščite vključujejo: nadzor aplikacij.
- Prepustnost požarne pregrade vsaj **27 Gbps** (tipa prometa: »Enterprise Traffic Mix«)
- Zaščite vključujejo: nadzor aplikacij, IPS.
- Prepustnost požarne pregrade vsaj **23 Gbps** (tip prometa: »Enterprise Traffic Mix«)
- Zaščite vključujejo: nadzor aplikacij, filtriranje spletnih vsebin, IPS, protivirusna zaščita, zaščita pred neznanimi ranljivostmi (ang.: 0-day), zaščita pred phishing napadi, zaščita pred napadi prek DNS protokola.
- Podpora vsaj 10M hkratnih sej.

- Podpora vsaj 300 000 novih sej na sekundo.

2.3.3. Tehnične zahteve požarne pregrade za strojno opremo:

Minimalne zahteve priklopa omrežnih vmesnikov ter strojne opreme posameznega člana gruče požarne pregrade:

- minimalno 8 x 10 GbE Base-F (SFP+) vmesnikov s priloženimi 6 x SFP+ moduli, z možnostjo razširitve do skupno 16 vmesnikov,
- minimalno 8 x 1GbE Base-T (RJ45) vmesnikov,
- podpora omrežnim vmesnikom 25 GbE (SFP28) do skupno 8,
- podpora omrežnim vmesnikom 40GbE Base-F (QSFP+) do skupno 4,
- Minimalno 2 x 900 GB SSD na posamezni procesni modul,
- Redundantno napajanje 100 – 240VAC
- Maksimalna višina strojne opreme 1 RU

2.3.4. Funkcionalne zahteve požarne pregrade:

- Podpora agregaciji omrežnih povezav 802.3ad.
- Podpora mehanizmom za usmerjanje:
 - OSPFv2 in v3,
 - BGP,
 - RIP,
 - PIM-SM, PIM-SSM, PIM-DM,
 - IGMP v2 in v3.
- Podpora za IPv6 protokol:
 - podpora funkcionalnostim: požarna pregrada, varnostno pregledovanje prometa (npr. filtriranje spletnih vsebin, IPS, nadzor aplikacij),
 - identifikacija uporabnikov.
- Identifikacija uporabnikov preko integracij:
 - Microsoft AD, Cisco ISE, SAML Identity Provider, Syslog, NetIQ eDirectory in ostalimi rešitvami, ki podpirajo tehnologijo Web API.
- Podpora avtentikacijskim shemam: žetoni (npr -SecureID), TACACS, RADIUS, digitalnim certifikatom, SAML.
- Podpora DHCP server in relay,
- Prepoznavanja in blokiranja prometa na nivoju aplikacij (vsaj: aplikacije za omogočanje oddaljene administracije, dostop do video vsebin, socialne medije, P2P, Anonymizer, škodljive aplikacije, visoko rizične aplikacije).
- Podpora prepoznavanju vsaj 6000 aplikacij, ki vključuje podporo tako IT kot OT aplikacij ter prepoznavanje podskupin posamezne aplikacije (baza aplikacij, ponujena s strani proizvajalca požarne pregrade).
- Priprava lastnega podpisa za določeno aplikacijo.
- Zaščita za odkrivanja in preprečevanje vdorov (IPS).

- IPS zaščita mora podpirati omrežne izjeme glede na vir, cilj, storitev ali kombinacijo treh.
- Samodejna aktivacija novih zaščit na podlagi nastavljenih parametrov (zmogljivosti, resnost grožnje, stopnja zaupanja, zaščita odjemalca, zaščita strežnika; ang.: performance impact, threat severity, confidence level, client protections, server protections).
- Možnost vnosa IOC-jev (Indicator Of Compromise) iz zunanjih virov (datoteka, HTTP, HTTPS,..).
- IPS zaščita mora omogočati mehanizem vklopa preko varnostnih profilov, ki jih je mogoče vezati na želene ščitene končne točke.

Ponujena rešitev mora vključevati varnostne zaščite NGFW:

- Sistem za preprečevanje vdorov (IPS): omogoča vključitev zaščite za odkrivanje in preprečevanje vdorov.
- Nadzor aplikacij: omogoča kontrolo uporabe posameznih ali kategorij IT kot OT omrežnih aplikacij.

2.3.5. Tehnične zahteve za centralni upravljalni sistem požarnih pregrad

Zahteve za centralni upravljalni sistem požarne pregrade podatkovnega centra:

- Upravljalni sistem mora licenčno omogočati upravljanje najmanj 2 enot požarnih pregrad (npr. 1 enota = 1 član gruča).
- Upravljalni sistem mora omogočati centralno upravljanje, konfiguracijo in nadzor požarnih pregrad (strojne in programske opreme).
- Minimalne zahtevane lastnosti programske opreme – upravljanje, logiranje in nadzor:
 - Omogočati mora spremljanje prometa in dogodkov v realnem času z možnostjo filtriranja vsaj po naslednjih parametrih: izvor, cilj, protokol, ciljni port, izvorni port.
 - Omogočati mora izdelavo varnostnih poročil ter korelacijo dogodkov periodično in na zahtevo.
 - Omogočati mora izdelavo varnostnih poročil za različna časovna obdobja (tedensko, mesečno, letno).
 - Omogočati mora centralno upravljanje (pisanje in nameščanje) varnostnih politik ter pripravo poročil iz enotne točke.
 - Omogočati mora pregled stanja posamezne požarne pregrade z vsaj naslednjimi parametri:
 - količina prometa, ki prehaja preko požarne pregrade,
 - število aktivnih in novih sej na požarni pregradi,
 - obremenitev sistemskih virov na požarni pregradi (CPU, RAM, ...),
 - stanje VPN povezav in količina prometa,
 - pravil na nivoju domenskega uporabnika, domenske uporabniške skupine,
 - Podpora upravljanju varnostnih pravil (npr. združevanje objektov v skupine, negiranje pogojev).
 - Prikaz, kolikokrat je bilo posamezno pravilo uporabljeno.

- Delo več administratorjev hkrati v načinu read-write ter preprečevanje spreminjanja istega objekta ali pravila.
- Možnost upravljanja varnostnih pravil preko API vmesnika.
- Podpora upravljanju objektov v varnostni politiki ter predefiniranih dinamičnih objektov znanih ponudnikov storitev (npr. Office 365, Amazon Web Services (AWS), Azure GEO).
- Omogočati mora pregledovanje dogodkov in dnevniških zapisov tudi preko brskalnika (npr. za potrebe SOC).
- Možnost nivojske administracije varnostne politike.
- Možnost pošiljanja dnevniških zapisov v SIEM sisteme preko različnih protokolov.
- Alarmiranje v primeru izpada posameznega modula požarne pregrade: SNMP, SMTP, Syslog.
- Upravljanje različic (revision control): pregled zgodovine različic varnostne politike in možnost vračanja na določeno različico ter njeno urejanje.
- Vgrajen MITRE ATT&CK framework.
- Dvonivojsko potrjevanje sprememb v varnostni politiki.

2.4 Zahteve za garancijo proizvajalca za strojno in programsko opremo

Podpora in vzdrževanje proizvajalca:

- Vključuje vse dopolnitve (angl. Latest Hot Fixes, Bug Fixes) in popravke (angl. Service Packs).
- Vse funkcionalne nadgradnje (angl. Feature Upgrades, Major Upgrades & Enhancements) ter vse nove izdaje in pod-izdaje (angl. Major and Minor Releases).
- Podpora s strani proizvajalca 24 ur na dan, vse dni v letu, posredno prek partnerja ali skrbnika sistema.
- Zagotovljen 4-urni odzivni čas (angl. Committed Response Time) za zadeve najvišje pomembnosti (angl. Severity 2, 3 & 4 issues), posredno prek partnerja ali skrbnika sistema.
- Dostop do forumov proizvajalca.
- Dostop do proizvajalčeve baze znanja.
- Možnost odprtja neomejenega števila servisnih zahtevkov brez dodatnih stroškov (posredno prek partnerja ali skrbnika sistema).
- Neposredna možnost spremljanja stanja odprtih servisnih zahtevkov.
- Dostop do informacij o vseh novostih, vključno z obvestili po elektronski pošti.

Programske storitve za sprotne posodobitve baze podpisov za varnostne grožnje:

- Vse posodobitve za zaščito pred informacijskimi grožnjami vseh licenciranih mehanizmov morajo biti na voljo za dobo trajanja podpore proizvajalca.

2.5 Storitve implementacije

Planiranje in dokumentacija:

- Izdelava visoko- in nizkonivojskega načrta s postavitvijo požarnih pregrad ter planirano vmesno fazo migracije iz obstoječe omrežne opreme

- Posodobitev obstoječe dokumentacije

Izdelava planov migracij sklopov seljenih segmentov

Namestitev nove strojne opreme:

- Osnovna priprava namenskih procesnih modulov ter namestitev priporočene programske različice na sisteme.
- Prenos modulov na lokacijo ter njihova vgradnja.
- Izvedba mrežnih povezav ter označb.
- Vklop opreme ter izvedba osnovnih testov delovanja:
 - Preverba delovanja mrežnih vmesnikov
 - Vklop izklop naprav
 - Pregled sistemskih dnevnikov

Nastavitve programske opreme:

- Dodajanje gruče požarnih pregrad na upravljalni sistem
- Optimizacija performančnih ter sistemskih nastavitev.
- Priprava nastavitev dinamičnega usmerjanja kjer je to zahtevano.
- Izvedba osnovnih varnostnih pravil z dovoljenim celotnim prometom
- Nastavitev SNMP za potrebe nadzora požarnih pregrad.

Izvedba migracije:

- Izvedba osnovnih testov povezljivosti pred migracijo.
- Usklajevanje potrebnih postopkov ter nastavitev s skrbnikom omrežne opreme, ki so potrebni pri vsaki migraciji.
- Izvedba migracije omrežnih segmentov na nove požarne pregrade.
- Kjer je možno se izvedejo delne migracije enega ali več omrežnih segmentov.
- Izvedba testov delovanja po vsaki migraciji, ter vseh morebitnih popravkov za zagotovitev delovanja vseh sistemov.

Izdelava varnostne politike:

- Selitev delov varnostne politike omrežnih segmentov preseljenih iz robne požarne pregrade ter po potrebi pretvorba in prenos v nov upravljalni sistem požarne pregrade.
- Izdelava varnostne politike na način postopnega uvajanja varnostnih pravil na osnovi dnevniških zapisov do končnega stanja, kjer je dovoljen samo želeni promet, ter uveljavljeno končno pravilo z zavračanjem ostalega prometa (»DROP ANY«)
- Vklop dostopovnih ter varnostnih mehanizmov Nadzora aplikacij ter IPS ter njihova optimalna nastavitve.

2.6 Storitve vzdrževanja

Tehnična podpora in servisna popravila za obdobje 5 let s strani partnerja za strojno in programsko opremo.

V okviru garancije izvajalec zagotavlja naročniku nemoteno delovanje sistema in odpravo napak v predvidenem obdobju. Po poteku garancijske dobe deluje sistem samostojno v enakem obsegu,

kot je predmet povpraševanja (izjema so funkcionalnosti vezane na naročnine, ki po poteku slednjih delujejo v zmanjšanem obsegu oz. ne delujejo).

Izvajalec mora zagotavljati dežurno službo, klicni center na katerega lahko naročnik v režimu 24/7 prijavi napake in spremlja njihov status ter potek reševanja. Za dostope do različnih baz znanja, posodobitev aplikacij in različic, pa naročnik ponuja ustrezno podporo proizvajalca (opisano spodaj).

V okviru garancije tako izvajalec zagotavlja naročniku naslednje elemente:

- diagnostiko vseh okvar v povezavi z varnostnim sistemom ter odprava napak na sistemu,
- zamenjavo okvarjene opreme (delna ali v celoti) ne glede na fizično ali funkcionalno okvaro,
- dobavo in nameščanje popravkov vse systemske programske opreme v primeru funkcionalnih (in fizičnih) okvar in odstopanj od specificirane ponujene opreme,
- možnost dostopa do popravkov, nadgradenj in novih različic systemske in nadzorne programske opreme pri proizvajalcu opreme,
- dostop do novih digitalnih podpisov/vzorcev novih napadov za storitev IDS/IPS (samodejno in ročno),
- dostop do novih digitalnih podpisov/vzorcev za storitev nadzor aplikacij (samodejno in ročno),
- pomoč in podporo pri reševanju tehničnih problemov na postavljenem sistemu (v rednem delovnem času),
- dostop do baz znanj pri proizvajalcu,
- odpiranje in spremljanje odprtih problemov v režimu 24/7,
- diagnostika in interpretacija statistik na zahtevo (6x letno),
- dostop do tehnične podpore pri proizvajalcu,
- 2x letno preventivni pregled delovanja opreme.

Odzivni časi:

- Urgentna podpora: < 4 ure,
- standardna podpora: < 8 ur,
- predvideni posegi: po dogovoru.

Razpoložljivost:

- Urgentna podpora: 24x7x365,
- standardna podpora: delavniki med 8.00–17.00,
- predvideni posegi: po dogovoru.

Odzivni čas – čas od prejete zahtevke za intervencijo s strani naročnika do trenutka, ko je izvedena prva prijava v informacijski sistem naročnika, iz česar je razvidno, da je izvajalec pristopil k diagnostiki in odpravi napake.

Urgentna podpora – obsega strokovno tehnično pomoč pri reševanju urgentnih primerov, ki zajemajo izpad ali nepravilno delovanje sistemov in posledično možnost gospodarske škode za DARS.

Standardna podpora – obsega strokovno tehnično pomoč pri reševanju težav na informacijskih sistemih in niso kritične narave, vseeno pa lahko ob predolgemu času reševanja ogrožajo poslovanje DARS-a.

Predvideni posegi – obsega strokovno podporo za posege, ki se odvijajo na sistemih in niso nujne narave. Posegi so vnaprej planirani v okviru minimalnega izpada delovanja sistema.

2.6.1. Lokacije naročnika

Naročnikovo okolje, ki je predmet razpisa, je postavljeno na dveh lokacijah:

- Ljubljana – Dragomelj – PDC (primarni podatkovni center)
- Ljubljana – Grič – RDC (sekundarni podatkovni center)

2.6.2. Povezljivost lokacij

Lokacije so povezane preko lastnih povezav (dark fiber). Povezave so rešene preko dveh ločenih tras.

Na nivoju omrežja je vzpostavljena L2 povezava med lokacijama PDC in RDC.

2.7 Specifikacija zahtevane dokumentacije

V nadaljevanju je seznam dokumentacije, ki jih v okviru projekta mora pripraviti ponudnik z namenom integracije vseh komponent, elementov in podsistemov v zanesljiv ter normalno, stabilno in pravilno delujoči sistem.

2.7.1. Izvedbeni načrt

S strani naročnika potrjen izvedbeni načrt je pogoj za začetek del. Izvedbeni načrt mora obsegati vsaj:

- Faze projekta
- Za vsako aktivnost v vsaki fazi opredelitev je treba podati:
 - Nosilca na strani ponudnika
 - Predviden čas dejavnosti (do ravni dneva)
 - Predvideno trajanje dejavnosti
 - Vpliv na delovanje storitev naročnikovega okolja
 - Tveganja in načini zmanjševanja le-teh
- Opis protokola testiranja in prevzema rešitve.
- Protokol komuniciranja (kontakti, način izmenjave dokumentacije, način varovanja podatkov, način poimenovanja dokumentacije in označevanje različic).

Načrt mora biti pripravljen v razpredelnični obliki (npr. format XLSX) s pripadajočim gantogramom.

2.8 Visokonivojska tehnična dokumentacija

S strani naročnika potrjena visokonivojska dokumentacija (HLD) je pogoj za začetek del. HLD mora podati arhitekturo rešitve in opredeliti glavne gradnike. HLD mora biti napisan v inženirsko-poljudnem jeziku, razumljivem širši množici informatikov.

HLD mora biti opremljen s shemami in razlagami le-teh. HLD mora opredeliti pojmovnik in kratice, ki se morajo konsistentno uporabljati v vsej dokumentaciji.

HLD mora biti pripravljen v formatu DOCX. Vse sheme morajo biti priložene v izvorni obliki.

2.8.1. Nizkonivojska tehnična dokumentacija

Nizkonivojska dokumentacija (LLD) mora slediti poglavjem iz HLD. V HLD opisana funkcionalnost mora v LLD biti opredeljena z vsemi parametri in morebitnimi dodatnimi razlagami. Vsebuje podroben tehnični načrt postavitve in konfiguracije strojne in programske opreme.

Dodatne razlage se lahko sklicujejo tudi na proizvajalčevo originalno dokumentacijo (ime dokumenta, stran in ime datoteke), ki mora biti priložena v obliki PDF. Izjemoma se lahko uporabi tudi sklicovanje na URL.

Dokumentirani morajo biti vsi parametri, ki nimajo privzetih vrednosti ali pa so bile le-te spremenjene. Privzete vrednosti je treba navesti tam, kjer so njihove navedbe smiselne zaradi razumevanja dokumenta.

Parametre, ki jih ponudnik ne more določiti (npr. IP-naslovi) mora ponudnik v LLD jasno označiti in pred začetkom del dobiti odgovore naročnika.

Arhitekturne odločitve morajo biti razrešene že v pripravi HLD. V primeru, da se pojavijo dodatna vprašanja o arhitekturi, jih mora ponudnik predstaviti naročniku in uskladiti rešitev.

LLD mora biti pripravljen v formatu XLSX z morebitnimi referencami na pojasnila v formatu DOCX.

2.8.2. Dokumentacija postopkov uvedbe, testiranja in upravljanje rešitve

Ponudnik mora pripraviti dokumentacijo za uvedbo in testiranje rešitve ter njeno upravljanje. Dokumentacija se mora smiselno sklicevati na HLD in predvsem na LLD in mora vključevati:

Dokumentacija postopkov prehoda na novi sistem. Dokument mora biti pripravljen v tabelarični obliki XLSX z morebitnimi referencami na DOCX. Dokument mora vsebovati:

- Glavne korake aktivnosti uvedbe rešitve
- Okvirno trajanje aktivnosti glavnih korakov
- Vpliv aktivnosti na delovanje storitev
- Načrt testiranja uspešnosti posamezne aktivnosti
- Način povrnitve v primeru neuspešne izvedbe aktivnosti
- Tveganja in načini zmanjševanja tveganj

Dokumentacija testnih scenarijev:

- Testiranje funkcionalnosti
- Testiranje sistema kot celote

Dokumentacija upravljanja rešitve:

- Dokumentacija postopkov okrevanja ob izgubi posameznega gradnika sistema
- Dokumentacija postopkov preklopa
- Dokumentacija ključnih operativnih postopkov (za systemske inženirje naročnika). Dokument naj se smiselno sklicuje na strani v proizvajalčevi dokumentaciji in HLD ter LLD.

Dokumenti so v obliki DOCX ali XLSX. XLSX se uporabi v primeru obsežnejših tabel s sklici na morebitne razlage v DOCX.

2.8.3. Izobraževanje

Ponudnik mora na lokaciji naročnika izvesti izobraževanje strokovnjakov naročnika za upravljanje in vzdrževanje sistema. V vseh fazah vzpostavitve novega sistema mora ponudnik omogočiti sodelovanje strokovnjakov naročnika z namenom uvajanja in prenosa potrebnih znanj.

Šolanje se izvede pod naslednjimi pogoji:

- Šolanje je neuradno.
- Šolanja se izvedejo v prostorih (predavalnici) naročnika.
- Šolanje se izvede v naročnikovem okolju.
- Ponudnik mora za prikaz delovanja uporabiti tudi lastni laboratorij (predvsem tam, kjer bi zaradi prikaza lahko prišlo do motnje v naročnikovem okolju).
- Obseg izobraževanja je omejeno na 1 (en) dan.

3. Izvedba pogodbenih obveznosti

3.1 Redno obratovanje

Ponudnik po izvedbi vseh storitev implementacije, vključno z namestitvijo ter konfiguracijo strojne in programske opreme, izvedbo storitev ter izdelavo končne dokumentacije izvedenih del, vzpostavi produkcijsko okolje in skupaj z naročnikom izvede tehnični pregled. O uspešno izvedenem tehničnem pregledu naročnik in ponudnik podpišeta zapisnik o prevzemu celotnega sistema v obratovanje v produkciji.

4. Ponudbeni predračun

Ponudnik:

PONUDBENI PREDRAČUN št.

Nakup, vzpostavitev in vzdrževanje požarne pregrade podatkovnega centra

Oznaka	Strojna oprema	ME	Količina	Cena/ME	Vrednost
A	Požarna pregrada	Kpl	2		
B	Programska oprema za upravljanje požarne pregrade	Kpl	1		
C	Storitev izvedbe	Kpl	1		
D	Mesečno vzdrževanje in odzivnost*	Mesec	60	750,00	45.000,00
E	Pomoč pri upravljanju	Ura	150		

*v skladu s točko 14.2 navodil je postavka D fiksirana in jo mora ponudnik upoštevati pri skupni vrednosti (skupaj A do E).

Skupaj A do E

DDV 22 %

Skupaj z DDV

Strinjamo se, da so razpisane količine na enoto mere in so okvirne ter se prilagajajo konkretnim potrebam ter razpoložljivim finančnim sredstvom naročnika. Naročnik ni zavezan naročiti celotne količine storitev.

Izjavljamo, da smo ponudili in izpolnili vse pozicije iz predračuna. Nobene od postavk ne ponujamo brezplačno, ni enaka 0 EUR ali neizpolnjena.

Vse cene in vrednosti so izražene v evrih. Cena ne vsebuje DDV. Cene in vrednosti so obračunane in zaokrožene na dve (2) decimalki. V ponudbeni ceni/ME so zajeti vsi stroški v zvezi s predmetom naročila.

Datum:

Podpis: