

SPECIFIKACIJE

Naročnik	AJPES Tržaška cesta 16 1000 Ljubljana
Oznaka javnega naročila	
Naziv javnega naročila	Izvajanje sistemskih storitev AJPES

1. VRSTA, LASTNOSTI, KAKOVOST IN IZGLED PREDMETA JAVNEGA NAROČILA/PONUDBE

OPIS STORITEV, KI SO PREDMET POGODBE
Ponudnik mora ponuditi vsa področja in vse storitve iz specifikacij v nadaljevanju. Oddaja ponudbe za posamezno področje ali storitve ni dopustna. <u>Področje 1: Storitve rednega vzdrževanja</u> a) Storitve upravljanja zaznave in odziva (Manage, detection and response - krajše MDR storitev) Ponudnik bo v okviru upravljanja storitev MDR moral zagotoviti, da bo MDR storitev vzpostavljena, pripravljena za delovanje in bo zagotavljala prehod in integracijo naslednjih naročnikovih orodij (v nadaljevanju »Defender«) v celovito storitev MDR na osnovi Microsoft Defender for Endpoint P2, Microsoft Defender for Identity in Entra ID Protection. MDR storitev obsega do 500 končnih točk in identitet. Ponudnik mora izvesti vse storitve, ki so potrebne za izvajanje storitve, od tega najmanj: • Vzpostavitev storitve MDR vključno z namestitvijo in nastavitvijo tehnološke platforme, ki vključujejo: delavnice za načrtovanje uvedbe storitev, podporo pri integraciji nadzornih tehnologij (Defender) znotraj definirane arhitekture, podporo pri načrtovanju procesov sodelovanja (npr. obveščanje o incidentih, odzivanje na incidente), ter zaključni pregled pripravljenosti okolja za začetek storitve MDR. • Izvajanje storitve upravljanega zaznavanja in odziva na grožnje (Managed Detection and Response – MDR), ki vključuje: ○ 24/7 nadzor varnostnih dogodkov in samodejno ter ročno triažiranje dogodkov na podlagi detekcijske logike in korelacijskih pravil; ○ preiskave zaznanih varnostnih dogodkov in incidentov, vključno z identifikacijo lažno pozitivnih ter klasifikacijo aktivnosti (npr. škodljiv, benign, lažno pozitiven);

- proaktivno iskanje znakov kompromisa (»threat hunting«) z uporabo analitičnega pristopa znotraj razpoložljivih podatkov;
- obveščanje in eskalacija incidentov predhodno določenim kontaktom;
- integracija virov obveščevalnih podatkov o grožnjah (»Threat Intelligence«) in posodabljanje zaznav na podlagi novih groženj in ranljivosti;
- zagotavljanje dostopa do varnostnih analitikov ponudnika za strokovno podporo in svetovanje znotraj delovnega časa ponudnika (8x5).
- izvajanje vnaprej dogovorjenih ukrepov za zaježitev incidentov na predhodno določenih sredstvih (kot na primer izolacija delovne postaje, onemogočitev uporabnika);
- stalno prilagajanje detekcijskih mehanizmov z namenom izboljšanja natančnosti in zmanjšanja lažnih alarmov;
- priprava mesečnih poročil in obravnava poročila na mesečnem sestanku o aktivnostih in ključnih incidentih in ugotovitvah, trendih in priporočilih. Na mesečnem sestanku poteka vsa komunikacija v slovenskem jeziku;
- Ponudnik omogoči naročniku dostop do spletnega portala, ki mora omogočati najmanj:
 - Zagotavljanje spremljanja obravnave varnostnih dogodkov od njihove zaznave do zaključka posameznega dogodka ali incidenta;
 - Vključevanje in komunikacija s strani izvajalca v primerih, ko za učinkovito obravnavo incidenta potrebuje dodatne informacije od naročnika;
 - Redno pregledovanje zaključenih incidentov in kibernetских varnostnih dogodkov za celotno obdobje trajanja pogodbe;
 - Omogočen dostop naročniku do vseh relevantnih podatkov v realnem času, nemudoma ob zaznavi varnostnega dogodka;
 - Zagotovitev pregleda nad izvajanjem vseh drugih zahtevkov, povezanih z izvajanjem pogodbenih storitev;
 - Vzpostavitev arhiva mesečnih poročil, ki bo dostopen naročniku skozi celotno trajanje pogodbe;
 - Možnost tiskanja in izvoza poročil o kibernetских dogodkih po različnih časovnih intervalih (dnevno, tedensko, mesečno, letno);
 - Priprava in omogočen pregled metrik, statističnih analiz ter trendov glede kibernetских dogodkov na dnevni, tedenski in mesečni ravni.

Redno izvajanje MDR storitev

Ponudnik mora zagotavljati neprekinjeno izvajanje storitev v režimu 24/7, s stalnim nadzorom, zaznavanjem ter obravnavo varnostnih dogodkov in incidentov. Storitve mora vključevati sprejem dogodkov, začetno odzivanje (zajezev) ter celovito obravnavo in zaključevanje varnostnih incidentov.

Pri tem mora ponudnik upoštevati čas preiskave, ki definira nivo storitve (SLA/KPI) definirane kot seštevek časa za zaznavo oz. začetek reševanja ter časa za izvedbo preiskave. Incident velja za preiskan, ko naročnik prejme poročilo o incidentu in je izveden začetni odziv oz. zajezev incidenta. Čas preiskave se šteje kot zaključen, ko ponudnik naročniku posreduje poročilo o incidentu. V primerih, ko potrditve incidenta ni mogoče zagotoviti brez dodatnih informacij, se čas preiskave zaključi ob posredovanju zahteve za pojasnilo naročniku. Varnostni dogodki, ki se obravnavajo kot lažno pozitivni in so kot taki tudi zaključeni, niso vključeni v izračun časa preiskave, saj zanje ni predvidena priprava poročila.

Povprečen čas preiskave glede na resnost incidentov mora biti:

- **Kritična resnost:** do 60 minut
- **Visoka resnost:** do 240 minut
- **Srednja resnost:** do 360 minut
- **Nizka ali informativna resnost:** po najboljših močeh (»best-effort«)

Ponudnik mora zagotavljati redno koordinacijo z naročnikom, spremljanje zahtevanih kazalnikov uspešnosti in znotraj lastnih procesov zagotavljati neprestano izboljševanje izvajanja storitve.

Kibernetška obveščevalna dejavnost o grožnjah (CTI)

Ponudnik mora pri izvajanju storitev aktivno uporabljati vire kibernetškega obveščanja (threat intelligence), z namenom pravočasnega zaznavanja in obvladovanja groženj. Uporabljeni morajo biti tako javni kot komercialni viri, ki vključujejo podatke o indikatorjih ogroženosti ter taktikah, tehnikah in postopkih napadalcev.

Avtomatizacija varnostnih operacij (SOAR)

MDR ponudnik mora imeti zmožnosti za avtomatizacijo odzivov na varnostne incidente (SOAR), kar obsega podporo za orkestracijo varnostnih orodij, avtomatizirane procese odzivanja ter upravljanje obravnave incidentov.

Odziv na kritične incidente s svojo CSIRT ekipo (Cyber Security Incident Response Team)

Ponudnik mora imeti zagotovljene zmožnosti za hitro in učinkovito obravnavo večjih varnostnih incidentov preko ustrezno usposobljene ekipe za odziv na kibernetške grožnje (CSIRT). Ekipo mora biti sposobna ukrepanja v primeru aktivnega napada, izvajanja digitalne forenzike ter izvedbe sanacijskih ukrepov. Zahtevane so praktične izkušnje in strokovno znanje na naslednjih področjih:

- Upravljanje in varovanje virtualizacijskih okolij (VMware, Hyper-V) ter strežniških operacijskih sistemov (Windows Server, Linux);
- Vzdrževanje in zaščita Microsoft oblačnega okolja (Azure);
- Upravljanje in zaščita domenskih storitev temelječih na Microsoft Active Directory tehnologiji;
- Upravljanje mrežne infrastrukture, vključno s konfiguracijo in zaščito stikal, usmerjevalnikov ter požarnih pregrad.

Varnost podatkov

Ponudnik mora zagotavljati izvajanje MDR storitev na decentraliziran način, pri čemer se uporabi orodje oz. portal Microsoft Defender, ki ga upravlja naročnik. V okviru takšnega pristopa ponudnik ne prenaša celotne podatkovne telemetrije zajete na podatkovnih virih v lastne sisteme. Ponudniku je dovoljen prenos podatkov v minimalnem obsegu o varnostnih dogodkih, zaznanih incidentih ter alarmih, ki so relevantni za obravnavo varnostnih tveganj. Prenos podatkov mora biti skladen z GDPR uredbo in ZVOP-2.

Takšen pristop omogoča višjo stopnjo nadzora nad podatkovnimi tokovi in skladnost z načelom najmanjšega potrebnega obsega podatkovnega prenosa. Ponudnik mora svojo rešitev prilagoditi temu varnostnemu modelu in zagotoviti, da obdelava podatkov poteka na način, ki ne vključuje centralnega zbiranja vseh virov telemetrije v lastnem okolju, temveč temelji na selektivnem pristopu obdelave dogodkov.

Področje 2: Sistemska dodatna dela po naročilu

Ponudnik bo po naročilu naročnika v okviru storitev izrednega vzdrževanja zadolžen za izvedbo dodatnih storitev iz področja rednega vzdrževanja.

b) Storitve tehnične podpore vzdrževanja in aktivno upravljanje WAF sistema - F5 BIG-IP

Ponudnik v okviru tehnične podpore vzdrževanja in aktivnega upravljanja WAF sistema - F5 BIG IP nudi:

- F5 BIG-IPi2600 Local Traffic Manager z dodatno nameščenima moduloma BIG-IP Application Security Manager Module for i2X00 in BIG-IP Access Policy Manager Base Module for i2600;
- dostop do novih verzij programske opreme in tehnoloških informacij,
- 1x (enkrat) letno na zahtevo namestitev nove verzije programske opreme pri naročniku (lahko preko oddaljenega dostopa).

Ponudnik zagotavlja naslednji SLA:

- Standardna sprememba: vnaprej avtorizirana sprememba, ki se lahko izvede neposredno brez potrebe po večjih spremembah delovanja ali arhitekturnih odločitvah, brez zahtev za dokumentacijo ali potrebe po servisnem oknu (menjava certifikata, konfiguracija novega VIPa...). Izvede se med delovnim časom (8x5, med 8:00 in 16:00, v roku 3 delovnih dni);
- Večja sprememba: pomeni zmerno tveganje ali re-konfiguracijo obstoječih storitev v produkcijskem okolju (spremembe na obstoječi konfiguraciji ali servisih, kjer lahko pride do izpada delovanja). Izvede se v dogovorjenem servisnem oknu, lahko med delovnim časom, če ni drugače navedeno v zahtevku za spremembo. Izvede se po postopkih, časovnem načrtu in dogovorjenih scenarijih testiranja (8x5, med 8:00 in 16:00, v roku 10 delovnih dni);
- Nujna sprememba: mora biti izvedena za rešitev kritičnega incidenta ali za izvedbo varnostnega popravka visoke resnosti (24x7 v 24 urah);
- Odzivni čas 60 minut;
- Dnevni monitoring delovanja okolja, servisov in storitev, ki jih F5 zagotavlja;
- Proaktivno zaznavanje in odpravljanje napak;
- Obveščanje naročnika o nepravilnem delovanju z namenom čim hitrejši odpravi napak;
- Zagotavljanje skladnosti rešitve s priporočili principala;
- Dodeljevanje in upravljanje pooblastil (dostopov);
- Priprava uporabniških navodil in izobraževanj uporabnikov (operativa, razvoj, sistem) o načinu dela in vzpostavljenih rešitvah, če je potrebno za zagotavljanje optimalnega upravljanja;
- Zagotavljanje izvajanja varnostnega kopiranja (obseg in urnik, periodično preverjanje obnovitev);
- Beleženje in zaščita revizijskih sledi o prijavah in spremembah na sistemu, alarmiranje ob incidentih (nepooblaščen dostop);
- Upravljanje varnostnih incidentov (analiza, poročilo), ki jih zazna F5;
- Pomoč razvojni in sistemski ekipi pri načrtovanju novih storitev z uporabo F5, kar vključuje visoko in nizkonivojsko arhitekturo rešitve;
- Pomoč razvojni in sistemski ekipi naročnika pri zaznavanju, analizi in odpravi kompleksnih težav z delovanjem storitev v okolju naročnika, katerih del je F5;
- Stalen prenos znanja o okolju in storitvah na delavce naročnika, ki sodelujejo pri razvoju novih storitev, odpravi napak na okolju F5 in v odpravi napak v širšem kontekstu zagotavljanja optimalnega delovanja storitev (omrežje, virtualno okolje in druge naprave naročnika - end-to-end);
- Mesečna delavnica: pregled alarmov in opozoril, pregled vzorcev napadov, pregled varnostnih dogodkov (block/alarm/learn), pregled varnostnih kršitev v načinu Staging (zabeleženo, transakcija ni blokirana) in Operational

– odprava lažnih alarmov (False Positive), pregled zaznanih in blokiranih http zahtevkov z namenom optimizacije pregledovalnika in izločanje manj pomembnih varnostnih dogodkov, dokumentiranje vsake spremembe ASM varnostne politike;

- Redna komunikacija in poročanje po dogovoru z naročnikom.
- 2x letno pregled za optimizacijo delovanja sistema in poročilo o predlogih sprememb/nadgradenj/optimizacije (HW in SW);
- Sprotno ažuriranje dokumentacije sistema in rešitev ob spremembah (change log);
- 1x letno posodobitev dokumentacije sistema in rešitev.

Dodatno še po posameznih modulih:

- Upravljanje modula F5 LTM: namestitev novih aplikacij in skrb za varno povezovanje (vključno z upravljanjem nameščenih certifikatov in uporabljenih naslovov IP), priprava kompleksnejših manipulacij prometa s pravili iRules in prilagojeno spremljanje delovanja in vzdrževanja kritičnih aplikacij po seznamu naročnika;
- Upravljanje F5 AWAf modula: zagotavljanje najvišjega nivoja varnosti za spletne aplikacije, ki jih želi naročnik zaščititi pred različnimi grožnjami. Podpora zaščite OWASPTop10, priprava podrobnejših in višjenivojskih pravil s kompleksnejšo zaščito za različne napade, tudi s sodelovanjem z naročnikovo razvojno ekipo aplikacij. Storitve vključuje pripravo in vzdrževanje varnostne politike napredne zaščite s podrobnim spremljanjem varnostnih dogodkov, pregledovanje vzorcev napadov in varnostnih kršitev ter odpravo lažnih alarmov.

Pri čemer naročnik zagotovi:

- razpoložljivost ključnih oseb za morebitna vsebinska in tehnična vprašanja;
- dostop do F5 okolja preko varne site-to-site VPN povezave.

Področje 2: Sistemska dodatna dela po naročilu

Ponudnik bo po naročilu naročnika v okviru storitev izrednega vzdrževanja zadolžen za izvedbo dodatnih storitev iz področja rednega vzdrževanja.

c) Storitve vzdrževanja in administracije Microsoft omrežnih storitev in produktov

Ponudnik v okviru vzdrževanja in administracije Microsoft omrežnih storitev in produktov zagotavlja podporo službi za informatiko naročnika in izvaja storitve vzdrževanja in administracije. Področja pričakovanih aktivnosti (storitev) so:

- Virtualizacija Hyper-V;

- Strežniška platforma na osnovi Windows server operacijskih sistemov;
- AD, DHCP in DNS omrežene storitve;
- Strežniške storitve (datotečni strežnik, tiskalniški strežnik);
- Poštni strežnik Exchange in spletni strežniki IIS;
- Microsoft 365 in Integracija On premise z Microsoft Cloud-om.

Podpora:

- Režim podpore 8/5 (ponedeljek–petek, delovni dnevi):
 - Odzivnost in sprejem zahtevka: do 2 h za incidente, do 8 h za spremembe, do 48 h za naloge;
 - Odprava napak oziroma priprava alternativne rešitve:
- Incidenti: Pri rešitvah, kjer proizvajalec ne zagotavlja delovanja ob odpovedih, nudimo odpravo napak po najboljših zmožnostih (»best-effort«);
- Spremembe in naloge: po dogovoru z naročnikom;
 - Planirane prekinitve iz naslova vzdrževanja so napovedane najmanj 8 dni vnaprej in so izvedene izven delovnega časa naročnika;
- Nadgradnje systemske programske opreme v okviru zmožnosti naročnikovega systemskega okolja in licenčne politike;
- Namestitve popravkov in varnostnih posodobitev na podprtih sistemih v okviru zmožnosti naročnikovega systemskega okolja in licenčne politike;
- Spremljanje in diagnostika delovanja sistemov;
- Proaktivno in preventivno ukrepanje za zagotavljanje nemotenega delovanja;
- Redna komunikacija in poročanje po dogovoru z naročnikom.

Administracija je zajeta v smislu 3. nivoja podpore.

Področje 2: Systemska dodatna dela po naročilu:

- spremljanje delovanja omrežnih storitev in produktov na podlagi dogovora z naročnikom,
- vzpostavitev (namestitve) omrežnih storitev in produktov,
- administracija, konfiguracija, konsolidacija in optimizacija omrežnih storitve in produktov,
- svetovanje in priprava predlogov naročniku,
- vodenje korespondence, poročanje in priprava systemsko tehnične dokumentacije,
- zagotavljanje razpoložljivosti ekipe za doseganje odzivnih časov naročnika glede na kategorizacijo in roke odprave napak,
- Izvedba dodatnih del po naročilu

d) Storitve vzdrževanja Oracle okolja

Ponudnik bo v okviru storitev vzdrževanja Oracle okolja prevzel vzdrževanje s celovitim procesom obravnave vseh zahtevkov in zagotavljanjem pogodbeno dogovorjene razpoložljivosti storitev (SLA). Aktivnosti bo izvajal na zahtevo naročnika v sklopu naročenih zahtevkov kontaktnega centra (Servicedesk).

Vključene storitve:

- Zagotavljanje razpoložljivosti in odprave napak v okoljih:
 - Linux strežniki,
 - Aplikacijski strežnik Oracle WebLogic & Forms,
 - Oracle podatkovna baza;
- Režim podpore 8/5 (ponedeljek–petek, delovni dnevi):
 - Odzivnost in sprejem zahtevka: do 2 h za incidente, do 8 h za spremembe, do 48 h za naloge,
 - Odprava napak oziroma priprava alternativne rešitve;
- Incidenti: Pri programskih rešitvah, kjer proizvajalec ne zagotavlja delovanja ob odpovedih, je dovolj odprava napak po najboljših zmožnostih (»best-effort«) v okviru zmožnosti redundantne arhitekture in licenčne politike naročnika;
- Spremembe in naloge: po dogovoru z naročnikom:
 - Planirane prekinitve iz naslova vzdrževanja so napovedane najmanj 8 dni vnaprej in so izvedene izven delovnega časa naročnika;
- Spremljanje in diagnostika delovanja sistemov;
- Proaktivno in preventivno ukrepanje za zagotavljanje nemotenega delovanja;
- Redna komunikacija in poročanje po dogovoru z naročnikom.

Področje 2: Sistemska dodatna dela po naročilu:

- Nadgradnje sistemske programske opreme v okviru zmožnosti naročnikovega sistemskega okolja in licenčne politike (Linux, Oracle WebLogic & Forms, Oracle DB);
- Namestitve popravkov in varnostnih posodobitev na podprtih sistemih v okviru zmožnosti naročnikovega sistemskega okolja in licenčne politike;
- Izvedba dodatnih del po naročilu.

e) Vzdrževanje računalniškega omrežja in omrežne opreme ter požarnih pregrad Check Point

Ponudnik bo v okviru izvajanja storitev vzdrževanja in sistemske podpore računalniškega omrežja in omrežne opreme zagotovil vzdrževanje ter sistemsko podporo za:

- 4x C9300x Cisco stikala (2 clustra in sicer 2 stikali v lokalnem data centru in 2 stikali v rezervnem data centru);
- 2x C9300 Cisco stikali (cluster v lokalnem data centru);

- 21 Cisco Meraki stikal 24 in 48 portnih, ki se nahajajo v centrali in v izpostavah;
- ter storitve sistema za dvo-faktorsko avtentifikacijo Cisco DUO;
- Področja pričakovanih storitev vzdrževanja ter sistemske podpore vzdrževanja omrežja se nanašajo na dogovorjene komponente in njihovo kategorizacijo. Izvajalec je dolžan zagotavljati podporo za:
 - poslovne povezave globalnega računalniškega omrežja in komunikacij (podpora vključuje komunikacijo s ponudniki internetnih storitev - ISP),
 - žično in brezžično lokalno računalniško omrežje,
 - komunikacijska in omrežna oprema, ter storitve primarnega podatkovnega centra,
 - komunikacijska in omrežna oprema, ter storitve rezervnega podatkovnega centra,
 - druge storitve iz področja omrežja in varnosti, ki jih definira naročnik.

Ponudnik bo v okviru vzdrževanja sistema požarnih pregrad Check Point s pripadajočimi licencami obsega zagotovil naslednje storitve vzdrževanja sistema v konfiguraciji:

- Gruča: 2 x Check Point CPAP-SG9100;
- samostojen Check Point CPAP-SG3600;
- Check Point Security Management CPSM-NGSM5.

Storitve vzdrževanja in podpore vključujejo:

- Zagotavljanje razpoložljivosti storitve klicnega centra ponudnika v režimu 8x5;
- Zagotavljanje razpoložljivosti tehnične ekipe za doseganje odzivnih časov naročnika glede na kategorizacijo napak:
 - kritična napaka je napaka, ki naročniku onemogoča poslovanje in katere izpad pomeni nedosegljivo storitev, ki jih nudi svojim naročnikom,
 - velika napaka je napaka, ki sicer omogoča omejeno delo zaposlenim, ali onemogoča delo omejenemu številu zaposlenim, ne vpliva pa na dosegljivo storitev za naročnike;
 - nekritična napaka je manjša motnja, ki vpliva samo omejeno na delo zaposlenih in ne vpliva na dosegljivost storitev za naročnike.
- Oddaljeno spremljanje delovanja aktivne omrežne opreme in skrb za arhiviranje konfiguracij omrežnih komponent;
- Odziv na morebitno nepravilno delovanje ali incidente;
- Redna komunikacija in poročanje po dogovoru z naročnikom.

Področje 2: Sistemska dodatna dela po naročilu:

- Administracija, konfiguracija, konsolidacija in optimizacija omrežnih storitve in opreme,
- odprava napak v delovanju računalniškega omrežja, omrežne opreme ter požarnih pregrad;
- Vodenje in usklajevanje aktivnosti z naročnikom in ostalimi deležniki;
- Svetovanje in priprava predlogov naročniku;
- Priprava sistemsko tehnične dokumentacije o konfiguraciji in administraciji omrežnega sistema;
- Oddaljena pomoč za uporabnike v odsotnosti lokalnega skrbnika;
- Izdelava mesečnih varnostnih poročil za področje CheckPoint;
- Izvedba dodatnih del po naročilu

f) Storitve svetovanja

Ponudnik bo v okviru izvajanja storitev svetovanja naročniku svetoval na različnih področjih IT arhitekture, IT infrastrukture, priprave optimizacije za optimalno delovanje in na področju načrtovanja izvedbe in priporočil.

Svetovanje na področju IT arhitekture

- Analiza obstoječe IT arhitekture;
- Presoja skladnosti arhitekture s poslovnimi cilji in dobrimi praksami, kar vključuje DevOps;
- Identifikacija arhitekturnih tveganj, podvajanj in neučinkovitosti;
- Priprava priporočil za ciljno (target) IT arhitekturo;
- Predlog arhitekturnih standardov in smernic za nadaljnji razvoj.

Svetovanje na področju IT infrastrukture

- Celovita presoja obstoječe infrastrukture (strežniki, omrežja, shranjevanje podatkov, virtualizacija, Kubernetes, DevOps);
- Varnostne rešitve, oblačne in hibridne rešitve);
- Upravljanje DNS zapisov preko platforme Cloudflare, ki vključuje konfiguracijo, nadzor, optimizacijo zmogljivosti ter zagotavljanje visoke razpoložljivosti, varnosti in zaščite pred DDoS napadi;
- Analiza zmogljivosti, razpoložljivosti, odpornosti in varnosti;
- Identifikacija ozkih grl, enojnih točk odpovedi in zastarelih tehnologij;
- Ocena stroškovne učinkovitosti in operative zrelosti infrastrukture.

Priprava optimizacije za optimalno delovanje

- Priprava optimizacijskega načrta za izboljšanje delovanja IT sistemov;
- Priporočila za izboljšanje učinkovitosti, zanesljivosti in razširljivosti;
- Predlogi za avtomatizacijo, standardizacijo in poenostavitev procesov;
- Priprava prioriteteznega seznama ukrepov z oceno koristi in tveganj.

Načrt izvedbe in strateška priporočila

- Priprava časovnega in izvedbenega načrta (roadmap);
- Opredelitev kratkoročnih, srednjeročnih in dolgoročnih aktivnosti;
- Ocena tveganj in predlogi omilitvenih ukrepov;
- Podpora naročniku pri odločanju in strateškem načrtovanju;
- Redna komunikacija in poročanje po dogovoru z naročnikom.

Ponudnik v ceno mesečnega pavšala vključi 10 svetovalnih ur na mesec.

Področje 2: SISTEMSKA DODATNA DELA PO NAROČILU

Ponudnik bo po naročilu naročnika v okviru storitev izrednega vzdrževanja zadolžen za izvedbo vseh dodatnih storitev s področja rednega vzdrževanja. Ponudnik lahko naroči dodatne svetovalne ure.

Storitve kontaktnega centra

Ponudnik bo v okviru storitev kontaktnega centra v upravljanje prevzel proces obravnave zahtevkov naročnika po področjih in sicer:

- Za Oracle vzdrževanje
- Za Check Point, Cisco in DUO vzdrževanje
- Za MDR, F5 in Microsoft vzdrževanje

Izvajalec mora:

- upoštevati tehnične in druge zahteve naročnika,
- vse podatke, pridobljene med in po izvedbi del, varovati kot zaupne,
- sodelovati s pooblaščenimi predstavniki naročnika in jih vključiti v vse faze priprave in uvajanja,
- ščititi interese naročnika in ga sproti pisno obveščati o vseh pomembnejših zadevah ali morebitnih problemih pri izvajanju pogodbenih del,
- zagotavljati storitve podpore skladno s pogoji navedenimi v osnutku pogodbe,
- ponudbo pripraviti v skladu s povabilom.

V ponudbenih vrednostih mora ponudnik upoštevati morebitne dajatve, materialne stroške, prevozne stroške in druge podobne stroške, ki so potrebni za izvedbo predmeta te pogodbe.

O podjetju Ajpes

AJPES ima 13 organizacijskih enot, določenih v Sklepu o ustanovitvi AJPES. Centrala ima sedež v Ljubljani, izpostave pa v naslednjih krajih: Ljubljana, Celje, Koper, Kranj, Krško, Maribor, Murska Sobota, Nova Gorica, Novo mesto, Postojna, Trbovlje in Velenje. Izpostave so I., II., in III. velikostnega razreda. Velikostni razred posamezne izpostave

je odvisen od števila vseh pravnih oseb in samostojnih podjetnikov na območju statistične regije, v kateri deluje izpostava.

Lokacija opravljanja storitev je centrala in izpostave AJPEŠ, Pošta Slovenije Maribor in na sedežu ponudnika. Podpora se vrši fizično na lokacijah ali oddaljeno prek VPN dostopa in oddaljenega dostopa na strežnike.

Pogodba:

Pogodba bo sklenjena za obdobje štirih (4) let.

Naročnik ima sklenjene naslednje pogodbe za isti predmet naročila z veljavnostmi:

1. Pogodba za področje MDR je sklenjena do konca decembra 2026.
2. Pogodba za področje F5 je sklenjena do konca decembra 2026.
3. Pogodba za področje Microsoft je sklenjena do konca decembra 2026.
4. Pogodba za področje Oracle je sklenjena do konca decembra 2026.
5. Pogodba za področje Cisco in Check Point je sklenjena do konca decembra 2026.
6. Pogodba za področje DUO je sklenjena do maja 2027.
7. Pogodba za področje storitve svetovanja do konca decembra 2026.

Prevzem posameznih storitev, ki se izvajajo po obstoječih pogodbah, bo izveden najkasneje ob izteku posamezne pogodbe. V primeru, če bo na javnem naročilu izbran trenutni ponudnik (če bo ta nastopal samostojno, v konzorciju ali kot podizvajalec), se ta z oddajo ponudbe strinja, da lahko naročnik obstoječo pogodbo prekine predčasno brez kakršnegakoli odškodninskega zahtevka, s trenutkom sklenitve pogodbe na podlagi tega javnega naročila. V primeru izbire drugega ponudnika bo izvajalec začel izvajati posamezne storitve s potekom obstoječih pogodb, pri čemer se storitve začnejo obračunavati sorazmerno z dnem začetka izvajanja prve od storitev glede na predračun.

Naročilo dodatnih storitev

Če se tekom trajanja pogodbe poveča število opreme pod vzdrževanjem, se sorazmerno poveča pavšalni znesek. Naročnik si pridržuje pravico, da tekom trajanja pogodbe skladno s prvo točko prvega odstavka 95. člena ZJN-3 naroči dodatne količine storitev, skupaj v višini največ 30% skupne pogodbene vrednosti brez DDV. Spremembo količin storitev naročnik s ponudniki ureja z aneksom k pogodbi. Smiselno enako bo naročnik storil v primeru, če se pojavi potreba po vzdrževanju novih tehnologij, ki jih bo naročnik kupil v času trajanja pogodbe oz. nadomestil obstoječe tehnologije z novimi. Novo tehnologijo bo naročnik smiselno umestil v enega od obstoječih področij storitev in obračunal po urni postavki za to storitev. Naročilo novih tehnologij naročnik s ponudniki ureja z aneksom k pogodbi na smiselno enak način.

Prav tako ima naročnik pravico tudi zmanjšati obseg storitev, če pride do spremembe vzdrževane opreme oz. uvedbe novih tehnologij.