

TEHNIČNE SPECIFIKACIJE

»OBNOVA IS OKOLJA, SERVER, VZDRŽEVALNE STORITVE«

1. PREDMET JAVNEGA NAROČILA

Predmet javnega naročila je celovita sanacija in nadgradnja obstoječega informacijskega oziroma strežniškega okolja naročnika, dobava in implementacija novega strežnika ter izvajanje sistemskega vzdrževanja za obdobje 36 mesecev.

Javno naročilo obsega:

1. pregled in analizo obstoječega stanja;
2. sanacijo ugotovljenih pomanjkljivosti;
3. izvedbo potrebnih konfiguracijskih in varnostnih ukrepov;
4. dobavo novega strežnika;
5. namestitev in konfiguracijo novega strežnika;
6. vključitev novega strežnika v obstoječe informacijsko okolje;
7. migracijo oziroma vzpostavitev potrebnih storitev;
8. preverjanje in vzpostavitev delovanja integracij z obstoječimi informacijskimi sistemi;
9. zagotavljanje podpore pri integraciji z informacijskim sistemom CADIS;
10. dokumentiranje izvedenih aktivnosti;
11. 36-mesečno sistemsko vzdrževanje;
12. odpravljanje sistemskih napak in incidentov;
13. izvajanje varnostnih posodobitev in drugih potrebnih vzdrževalnih aktivnosti;
14. podporo naročniku pri sistemskih vprašanjih in težavah.

Naročilo je zasnovano kot celovita storitev, katere cilj je zagotoviti stabilno, varno in vzdrževano strežniško okolje naročnika.

2. NAMEN IN CILJI NAROČILA

Namen naročila je zagotoviti:

1. sanacijo obstoječega strežniškega okolja;
2. odpravo obstoječih tehničnih in konfiguracijskih pomanjkljivosti;
3. vzpostavitev nove oziroma nadgrajene strežniške infrastrukture;
4. zanesljivo delovanje informacijskih sistemov naročnika;
5. ustrezno raven informacijske in kibernetske varnosti;
6. kontinuiteto delovanja ključnih informacijskih storitev;
7. ustrezno podporo uporabnikom;
8. ustrezno vzdrževanje strežniške infrastrukture;
9. obvladovanje tveganj, povezanih z informacijsko in kibernetsko varnostjo.

Pri izvedbi mora izvajalec upoštevati veljavno zakonodajo in druge predpise s področja informacijske in kibernetske varnosti, vključno z ZInfV-3, v delu, ki je relevanten za naročnika in predmet naročila.

ZInfV-3 ureja področje informacijske in kibernetske varnosti ter med drugim določa ukrepe za obvladovanje tveganj za informacijsko in kibernetsko varnost.

3. PREGLED OBSTOJEČEGA STANJA

Izvajalec mora pred izvedbo sanacije in implementacije novega strežnika opraviti pregled obstoječega informacijskega okolja naročnika.

Pregled mora obsegati najmanj:

1. pregled obstoječe strežniške infrastrukture;
2. pregled operacijskih sistemov;
3. pregled sistemskih servisov;
4. pregled uporabniških računov;
5. pregled uporabniških in administratorskih pravic;
6. pregled omrežnih nastavitev;
7. pregled varnostnih nastavitev;
8. pregled sistema varnostnega kopiranja;
9. pregled posodobitev;
10. pregled sistemskih dnevnikov;
11. pregled povezav z drugimi informacijskimi sistemi;
12. pregled integracij;
13. pregled integracije z informacijskim sistemom CADIS;
14. identifikacijo kritičnih oziroma potencialno kritičnih točk.

Po opravljenem pregledu mora izvajalec naročniku predstaviti ugotovitve in predlagane ukrepe.

4. SANACIJA OBSTOJEČEGA STANJA

Sanacija obstoječega stanja vključuje najmanj:

1. projektna priprava, inventarizacija in priprava ciljnega tehničnega načrta;
2. postavitve in hardening novega fizičnega Hyper-V strežnika;
3. postavitve dveh virtualnih strežnikov Windows Server 2022/2025;
4. migracija oziroma reorganizacija obstoječih strežniških vlog in podatkov;
5. uvedba in tehnična uveljavitev AD Tiering modela (Tier 0, Tier 1 in Tier 2);
6. ločevanje administratorskih identitet ter ureditev privilegiranih dostopov;
7. pregled in hardening servisnih računov ter uporaba gMSA, kjer je izvedljivo;
8. uvedba oziroma dokončanje Windows LAPS;
9. Active Directory, DNS in Group Policy hardening;
10. Windows Firewall, RDP, SMB, WinRM, TLS/SSL in SNMP hardening;
11. dodatna omrežna segmentacija in omejitev administrativnih komunikacij;
12. odprava preostalih ranljivosti, ki zahtevajo patching, upgrade ali firmware/driver posodobitve;
13. ureditev varnostnih kopij, obnovitvenih postopkov in testnega restore-a;
14. ureditev centralnega beleženja pomembnih varnostnih dogodkov in monitoringa, kjer je na voljo;
15. zaključna tehnična in varnostna dokumentacija.

Izvajalec mora vse pomembne spremembe ustrezno dokumentirati.

5. DOBAVA NOVEGA STREŽNIKA

Izvajalec mora dobaviti nov strežnik, ki je nov, nerabljen in namenjen profesionalni uporabi.

Strežnik mora biti primeren za neprekinjeno oziroma poslovno kritično delovanje in mora izpolnjevati vse zahteve, navedene v tehnični specifikaciji tega naročila.

5.1 Tehnična specifikacija strežnika

Količina (kos)	Opis
1	Ohišje 2U 24x2,5"
1	Izbira načina delovanja za: "Način največje učinkovitosti"
1	Procesor AMD EPYC 9115 16C 125W 2,6 GHz
2	64GB TruDDR5 6400MHz (2Rx4) RDIMM-A v2
1	raid kontroler z podporo za priklop 16 diskov in 4GB delovnega pomnilnika
4	trdi disk 2,5" VA 1,6TB Mixed Use SAS 24Gb HS SSD
2	trdi disk 2,5" VA 480GB Read Intensive SATA 6 Gb HS SSD v2
5	trdi disk 2,5" VA 1,92 TB Read Intensive SATA 6 Gb HS SSD v2
1	mrežna kartica Broadcom 5719 1GbE RJ45 4-port OCP Ethernet adapter
2	napajalnik 750W 230V Titanium Hot-Swap Gen2 napajalnik v3
2	2,8 m, 13A/100-250V, C13 na C14 premostitveni kabel
5	2U V3 Performance ventilatorski modul
1	komplet drsnih vodil
1	TPM 2.0
1	Laser indikator servisiranja
1	management s podporo za remote dostop, firmware nadgradnje, itd.
1	programska oprema za upravljanje strežnika s 5-letno garancijo za programsko opremo in podporo
1	5-letna standardna garancija

Kjer so v tehnični specifikaciji navedeni proizvajalec, blagovna znamka, tip ali poimenovanje, značilno za določenega proizvajalca, se šteje, da je dopustna tudi enakovredna rešitev, ki izpolnjuje enake ali boljše tehnične zahteve (»ali enakovredno«). Enakovrednost dokazuje ponudnik s tehničnim listom ponujenega strežnika.

6. DOBAVNI ROK

Izvajalec mora novo strežniško opremo dostaviti na lokacijo naročnika najkasneje v roku 10 koledarskih dni od podpisa pogodbe.

Rok začne teči naslednji dan po podpisu pogodbe oziroma skladno z določili pogodbe.

V roku dobave mora biti strežnik fizično dostavljen na lokacijo naročnika.

7. NAMESTITEV IN IMPLEMENTACIJA

Izvajalec mora po dobavi izvesti:

1. fizično namestitev strežnika;
2. priklop strežnika;
3. osnovno konfiguracijo;
4. namestitev operacijskega sistema;
5. namestitev potrebne programske opreme;

6. konfiguracijo omrežnih nastavitev;
7. konfiguracijo uporabnikov;
8. konfiguracijo administratorskih pravic;
9. konfiguracijo sistemskih servisov;
10. konfiguracijo varnostnih nastavitev;
11. vključitev v obstoječe okolje;
12. vzpostavitev potrebnih povezav;
13. vzpostavitev oziroma migracijo potrebnih storitev;
14. testiranje delovanja.

8. MIGRACIJA

Izvajalec mora zagotoviti prenos oziroma vzpostavitev vseh storitev in podatkov, ki jih naročnik potrebuje za nadaljnje nemoteno poslovanje.

Pred izvedbo migracije mora izvajalec:

1. pripraviti načrt migracije;
2. identificirati storitve in podatke, ki se migrirajo;
3. opredeliti tveganja;
4. določiti način varovanja podatkov;
5. po potrebi pripraviti povratni načrt;
6. izvesti migracijo;
7. preveriti pravilnost prenosa;
8. izvesti funkcionalne teste.

Po izvedeni migraciji mora izvajalec skupaj z naročnikom preveriti delovanje ključnih informacijskih storitev.

9. INTEGRACIJA Z INFORMACIJSKIM SISTEMOM CADIS

Izvajalec mora zagotoviti ustrezno podporo pri delovanju obstoječe integracije z informacijskim sistemom CADIS.

Storitev vključuje najmanj:

1. preverjanje obstoječe integracije;
2. podporo pri migraciji;
3. preverjanje delovanja integracije po migraciji;
4. odpravljanje napak na strežniškem oziroma sistemskem delu integracije;
5. podporo pri spremembah konfiguracije;
6. sodelovanje pri odpravljanju incidentov;
7. testiranje delovanja integracije po pomembnejših spremembah.

Izvajalec mora pri posegih v strežniško okolje zagotoviti, da zaradi izvedenih del ne pride do nedopustnega izpada oziroma nepravilnega delovanja integracije.

10. SISTEMSKO VZDRŽEVANJE

Izvajalec mora zagotavljati sistemsko vzdrževanje za obdobje 36 mesecev.

Vzdrževanje začne teči po uspešni vzpostavitvi in prevzemu novega strežniškega okolja oziroma na datum, določen v pogodbi.

10.1 Preventivno vzdrževanje

Preventivno vzdrževanje vključuje najmanj:

1. spremljanje delovanja strežnika;
2. pregled sistemskih dnevnikov;
3. pregled sistemskih servisov;
4. pregled zmogljivosti;
5. pregled porabe pomnilnika;
6. pregled diskovnih kapacitet;
7. pregled stanja diskov;
8. preverjanje varnostnih kopij;
9. preverjanje posodobitev;
10. preverjanje varnostnih nastavitev;
11. opozarjanje naročnika na ugotovljene težave;
12. priporočila za izboljšave.

10.2 Korektivno vzdrževanje

Korektivno vzdrževanje vključuje odpravljanje:

1. nedelovanja strežnika;
2. nedelovanja sistemskih servisov;
3. sistemskih napak;
4. težav z uporabniškimi pravicami;
5. težav z administratorskimi pravicami;
6. težav z omrežno povezljivostjo;
7. konfiguracijskih napak;
8. težav pri integracijah;
9. težav, povezanih z informacijskim sistemom CADIS, kadar se nanašajo na strežniško oziroma sistemsko okolje;
10. drugih napak, ki vplivajo na delovanje informacijskega okolja naročnika.

11. VARNOSTNO VZDRŽEVANJE

Izvajalec mora v času trajanja vzdrževanja izvajati oziroma zagotavljati:

1. varnostne posodobitve;
2. kritične sistemske popravke;
3. odpravljanje znanih ranljivosti;
4. preverjanje varnostnih nastavitev;
5. priporočene popravke proizvajalca;
6. spremljanje življenjskega cikla ključnih komponent;
7. opozarjanje naročnika na pomembna varnostna tveganja.

Če izvajalec zazna varnostno ranljivost, ki bi lahko pomembno vplivala na naročnika, mora o tem naročnika obvestiti brez nepotrebnega odlašanja.

12. SLA – ODZIVNI ČASI

Za potrebe vzdrževanja se določijo naslednje kategorije incidentov:

Prioriteta	Opis	Odzivni čas
P1 – kritično	Popolna nedostopnost ključnega sistema ali strežnika oziroma napaka, ki onemogoča bistveno poslovanje	največ 1 ura na lokaciji naročnika
P2 – visoko	Pomembna funkcionalnost ne deluje, vendar sistem kot celota deluje	največ 4 ure
P3 – običajno	Napaka z omejenim vplivom na poslovanje	največ 1 delovni dan
P4 – zahteva	Zahteva za spremembo, svetovanje ali manjši poseg	največ 2 delovna dneva

12.1 Kritični incident

Pri incidentu P1 mora izvajalec zagotoviti odziv najkasneje v eni uri.

Če reševanje incidenta zahteva fizično prisotnost, mora izvajalec zagotoviti prihod ustrezno usposobljenega strokovnjaka na lokacijo naročnika najkasneje v eni uri od prijave kritičnega incidenta.

Za odziv se šteje začetek dejanskega obravnavanja incidenta.

13. LOKACIJA IZVAJANJA STORITEV

Storitve se izvajajo:

1. na lokaciji naročnika;
2. po potrebi na daljavo, kadar to omogoča naročnik;
3. na drugih lokacijah, če je to potrebno za izvedbo storitve in je predhodno usklajeno z naročnikom.

Pri kritičnih incidentih lahko naročnik zahteva fizično prisotnost izvajalca na lokaciji.

Okvirno uporabniško okolje naročnika obsega približno 30 zaposlenih oziroma uporabnikov.

14. PREVZEM

Po zaključeni implementaciji mora izvajalec izvesti funkcionalno testiranje.

Prevzem se izvede, ko:

1. je strežnik nameščen;
2. je ustrezno konfiguriran;
3. so izvedene zahtevane migracije;
4. delujejo zahtevane sistemske storitve;
5. delujejo zahtevane integracije;
6. je preverjeno delovanje informacijskega sistema CADIS v delu, ki je predmet naročila;
7. je naročniku predana dokumentacija;
8. so odpravljene bistvene napake.

O uspešnem prevzemu se sestavi primopredajni zapisnik.

15. INFORMACIJSKA IN KIBERNETSKA VARNOST

Izvajalec mora pri izvedbi naročila upoštevati načela informacijske in kibernetske varnosti.

Izvajalec mora zlasti:

1. varovati podatke naročnika;
2. preprečevati nepooblaščen dostop;
3. uporabljati ustrezno zaščitene administratorske dostope;
4. varovati uporabniške in administratorske račune;
5. izvajati ustrezne varnostne posodobitve;
6. zagotavljati sledljivost pomembnih administrativnih posegov;
7. naročnika obvestiti o pomembnih varnostnih incidentih;
8. varovati dokumentacijo in konfiguracijske podatke;
9. po zaključku posameznega posega odstraniti začasne dostope, kadar niso več potrebni.

16. VAROVANJE PODATKOV

Izvajalec mora vse podatke, do katerih dostopa pri izvajanju pogodbe, uporabljati izključno za namen izvajanja pogodbenih obveznosti.

Izvajalec ne sme podatkov naročnika:

1. kopirati brez potrebe;
2. posredovati tretjim osebam;
3. uporabljati za druge namene;
4. hraniti dlje, kot je potrebno za izvedbo pogodbenih obveznosti.

Če izvajalec pri izvajanju storitev obdeluje osebne podatke, mora ravnati skladno z veljavno zakonodajo s področja varstva osebnih podatkov.

17. DODATNE STORITVE

Naročnik lahko izvajalcu po potrebi naroči tudi dodatne storitve, ki niso vključene v osnovni obseg pogodbenih storitev.

Izvajalec za vsako zahtevo naročnika za dodatne storitve najkasneje v treh delovnih dneh od prejema zahteve, če ni pisno dogovorjeno drugače, pripravi pisno ponudbo z opisom storitve, oceno potrebnega obsega ur in ceno. Naročnik ponudbo pisno potrdi ali zavrne. Potrditev ponudbe je pogoj za začetek izvajanja dodatne storitve. Če izvajalec dodatno storitev izvede brez predhodnega pisnega naročila naročnika, nosi stroške izvedbe sam.