



Vzdrževanje systemske infrastrukture eZdravja

TEHNIČNE SPECIFIKACIJE

Kazalo vsebine

1	Uvod	4
1.1	Definicije in okrajšave	4
2	Splošne zahteve in opis informacijske rešitve	5
2.1	Opis informacijske rešitve	5
2.1.1	Interoperabilna hrbtenica	5
2.1.2	Računalniško omrežje zNET	6
2.2	Gradniki interoperabilne hrbtenice in računalniškega omrežja	7
2.3	Obseg projekta	8
3	Predmet javnega naročila	9
3.1	Osnovno vzdrževanje	9
3.1.1	Vzdrževanje opreme proizvajalca Cisco	11
3.1.2	Vzdrževanje opreme proizvajalca Check Point	12
3.1.3	Upravljanje kontejnerskega okolja Red Hat OpenShift	12
3.1.4	Upravljanje virtualizacijskega okolja Linux in OLVM	13
3.1.5	Upravljanje sistemov IBM Storage Scale in Hashicorp Vault	13
3.1.6	Upravljanje podatkovnih baz na strojni opremi Exadata X11M Compute	14
3.2	Dopolnilno vzdrževanje	14
3.2.1	Dopolnilno vzdrževanje predvidoma zajema:	14
3.2.2	Dopolnilno vzdrževanje SDWAN zajema:	15
3.2.3	Dopolnilno vzdrževanje SIEM zajema:	15
3.2.4	Dopolnilno vzdrževanje v okviru zagotavljanja odzivne skupine CSIRT:	15
3.2.5	Ostale storitve dopolnilnega vzdrževanja	16
3.3	Storitev operativnega centra kibernetnega varovanja	16
3.3.1	Vzdrževanje sistema SIEM	16
3.3.2	Izvajanje storitev varnostno operativnega centra - SOC	17
3.4	Zagotavljanje kontaktnega centra in koordinacija reševanja zahtevkov	18
3.5	Izvajanje storitvenih zahtevkov, vodenje evidenc, koordinacija, poročanje in spremljanje obsega izvedenih del	19
3.5.1	Izvajanje storitvenih zahtevkov	20
3.5.2	Vodenje evidenc in poročanje	21
3.5.3	Koordinator izvedbe	23
3.5.4	Spremljanje obsega izvedenih del v okviru osnovnega vzdrževanja	24
3.6	Nadzor nad delovanjem informacijske rešitve	26
3.7	Licence za potrebe vzdrževanja infrastrukture eZdravja in omrežja zNET	27
3.7.1	Digitalna potrdila (certifikati)	28
3.8	Varnostne in tehnološke zahteve ter zagotavljanje odzivnih časov (SLA)	28

3.8.1	Varnostne zahteve.....	28
3.8.2	Tehnološke zahteve.....	30
3.8.3	Odzivni časi in zagotavljanje SLA.....	30
3.9	Postopki ob prevzemu in predaji del.....	35
3.10	Zagotavljanje potrošnega materiala in digitalnih potrdil.....	36
Priloga 1: Storitve vzdrževanja in upravljanja omrežja zNET.....		37
Upravljanje fizičnega in logičnega nivoja omrežja.....		37
Procesi upravljanja fizičnega in logičnega sloja omrežja zNET		37
Upravljanje in zagotavljanje delovanja varnega sistema oddaljenega dostopa do omrežja		39
Procesi upravljanja in zagotavljanja delovanja varnega oddaljenega dostopa do omrežja zNET		40
Upravljanje in zagotavljanje varnostnih sistemov v omrežju		41
Procesi upravljanja in zagotavljanja delovanja varnostnih sistemov v omrežju zNET:		42
Upravljanje in zagotavljanje pomožnih servisov za delovanje omrežja.....		43
Procesi upravljanja in zagotavljanja pomožnih servisov za delovanje omrežja zNET:		44
Priloga 2: Zaprti / zaupni del tehničnih specifikacij		46
Priloga 3: Potrošni material in digitalna potrdila		47

1 Uvod

Dokument predstavlja tehnične specifikacije za izvedbo javnega naročila »Vzdrževanje systemske infrastrukture eZdravja« in se sestoji iz javnega dela in zaupnega / zaprtega dela dokumentacije, ki ga predstavlja celotna kosovnica opreme z navedbo modelov opreme s serijskimi številkami, podrobnosti o režimu podpore, ipd.

Ker zaupni/zaprti del dokumentacije predstavlja poslovno skrivnost, njegovi podatki pa se ne razkrivajo javno tudi iz varnostnih razlogov, bo naročnik ta del dokumentacije zainteresiranim ponudnikom poslal na zahtevo ob predložitvi podpisane izjave "P-10: Izjava o varovanju zaupne dokumentacije / Potrdilo naročnika", skladno s postopkom, opredeljenim v Navodilu ponudnikom predmetnega javnega naročila.

V nadaljevanju se nahaja javni del Tehničnih specifikacij. Pri tem so v specifikacijah uporabljene definicije, akronimi in kratice, opredeljene v nadaljevanju.

1.1 Definicije in okrajšave

Definicije:

eZdravje	Nacionalna rešitev eZdravje z učinkovito obliko elektronskih rešitev prinaša večjo varnost in kakovost izvajanja zdravstvenih storitev.
IT rešitev	Skupek strojne in programske opreme, ki zagotavljanje informacijsko podporo poslovnim procesom (v besedilu se smiselno uporablja tudi beseda rešitev).
IT storitev	IT rešitev, skupaj s storitvami upravljanja
Ponudnik	Pravna oseba oziroma skupina pravnih oseb, ki se prijavlja na predmetno javno naročila. V nadaljnjem besedilu se namesto »ponudnik« uporablja tudi beseda »izvajalec«.

Okrajšave:

CRPP	Centralni register podatkov o pacientih
CSV	Comma-separated Values (z vejico ločeni podatki)
API	Application Programming Interface (Aplikacijski programski vmesnik)
IHE	Integrating the Healthcare Enterprise®
ISI	Informacijski sistem izvajalca
MZ	Ministrstvo za zdravje RS
NIJZ	Nacionalni inštitut za javno zdravje
PDF	Portable Document Format
PPOP	Povzetek podatkov o pacientu
PRC	Podatkovno računalniški center
OS	Operacijski sistem
SAM	Security Account manager
SIEM	Upravljanje varnostnih informacij in dogodkov (ang: Security Information and Event Management)
SNMP	Splošna nujna medicinska pomoč
SOC	Varnostno operativni center (ang. Security Operations Center)
SSO	Single Sign On (Enkratna prijava uporabnika)
TLS	Transport Layer Security
PK	Profesionalna kartica zdravstvenega zavarovanja
KZZ	Kartica zdravstvenega zavarovanja
ZZZS	Zavod za zdravstveno zavarovanje Slovenije

2 Splošne zahteve in opis informacijske rešitve

V tem poglavju je predstavljeno obstoječe stanje informacijske rešitve eZdravja, ki je predmet vzdrževanja, s ciljem ponudnikom krovno orisati področja in obseg javnega naročila, med tem ko se razpisne zahteve nahajajo v poglavju 3 – Predmet javnega naročila.

2.1 Opis informacijske rešitve

Informacijska rešitev se sestoji iz dveh ključnih delov, in sicer INTEROPERABILNE HRBTENICE in RAČUNALNIŠKEGA OMREŽJA zNET, ki sta podrobneje opisana v nadaljevanju.

2.1.1 Interoperabilna hrbtenica

Interoperabilna hrbtenica je skrajšan naziv za informacijsko tehnološko interoperabilno hrbtenico informacijskega sistema eZdravje. Interoperabilna hrbtenica predstavlja temeljno rešitev eZdravja, saj vzpostavlja osnovo za medsebojno povezovanje heterogenega okolja izvajalcev zdravstvene dejavnosti (IZD). Sestavljena je iz dveh večjih funkcionalnih sklopov (funkcionalnih komponent) oziroma dveh IT storitev:

- centralna strežniška in diskovna infrastruktura, in
- centralna baza podatkov.

Interoperabilna hrbtenica vključuje:

- celotno centralno strežniško in diskovno infrastrukturo ter sistemsko programsko opremo, namenjeno za potrebe projekta centralne baze podatkov ter posameznih programskih rešitev eZdravja,
- centralno bazo podatkov (CBP) na sistemskem nivoju, ki je namenjena za potrebe:
 - o delovanja IHE platforme (repozitoriji, EZZ in centralni indeks, delovne baze, ...);
 - o vzpostavitve centralnih registrov (register zdravil, register zdravstvenih storitev register izvajalcev zdravstvene dejavnosti, register pacientov, ...);
 - o za potrebe delovanja posameznih aplikacij (kot npr. eRecept, eNaročanje, CRPP, ...);

Funkcionalnosti, implementirane znotraj CBP interoperabilne hrbtenice, so naslednje:

- enotna podatkovna baza (database), ki omogoča generiranje posameznih, funkcionalno samostojnih baz (tablespace), katere morajo biti na ločenem diskovnem prostoru,
- omogočanje revizijskega sledenja in zapisovanje revizijskih sledi na varen način in na način, ki omogoča rekonstrukcijo vseh dogodkov (za ta namen je v okviru interoperabilne hrbtenice vzpostavljena enotna sinhronizacija časa):
 - o vseh pomembnejših dogodkov (dostopov do podatkovne baze in podatkov - tudi neuspešno izvedenih),
 - o vseh sprememb podatkov in
 - o vseh vpogledov v podatke.
- sposobnost repliciranja na dve različni mesti v podatkovno-računalniška centra (PRC):
 - o PRC 1 (Ljubljana): Stegne 19, 1000 Ljubljana;

- PRC 2 (Maribor): Zagrebška cesta 106, 2000 Maribor;
- sposobnost avtomatičnega preklopa na rezervno podatkovno bazo v primeru nedelovanja primarne lokacije,
- možnost varnostnega kopiranja (ang. backup) in obnovitve podatkovne baze, tako na nivoju celotne baze kot tudi posameznih logičnih baz,
- uporaba Unicode kodnega zapisa,
- ločitev upravljaljske (administratorske) in varnostne (security) funkcije,
- šifriranje podatkov (transparentno) tako na nivoju tabel, kot tudi na nivoju stolpcev,
- centralizirano upravljanje, diagnostika in orodje za optimizacijo delovanja centralne baze podatkov,
- omogočanje obnovitve stanja (restore) v določeni časovni točki (point in time) tako na sekundarni lokaciji kot pri obnovitvi iz varnostnih kopij.

2.1.2 Računalniško omrežje zNET

Varno zdravstveno omrežje zNET je komunikacijska infrastruktura, tako za centralizirane IT storitve nacionalnega pomena, kakor tudi za storitve IT, ki jih zagotavljajo posamezni akterji v zdravstvu prek certificiranih točk. Omrežje zNET zagotavlja varne in zanesljive povezave med vstopno točko, drugimi certificiranimi točkami in ključnimi akterji v zdravstvu.

Omrežje zNET ne vključuje lokalnih omrežij posameznih končnih točk ter sistemov (strežnikov in drugih naprav), ki so povezani na ta lokalna omrežja. Meja upravljanja omrežja zNET je vmesnik vstopne opreme omrežja zNET proti lokalnemu omrežju.

V zNET omrežje je trenutno vključenih več kot 400 izvajalcev zdravstvene dejavnosti (bolnišnice, zdravstveni domovi, koncesionarji,...).

Lastnosti omrežja zNET:

- omrežje zNET je zgrajeno iz samostojnih gradnikov in realiziranih na fizični opremi v upravljanju NIJZ,
- končne lokacije se lahko povezujejo v omrežje zNET preko treh ločenih logičnih povezav, ki se zaključujejo na centralni lokaciji in redundantni lokaciji,
- omrežje zNET ima zagotovljeno ločevanje administrativnih in uporabniških dostopov, zagotovljeno ločevanje dostopov do storitev, zagotovljeno ločevanje dostop med članicami omrežja in zagotovljen ustrezen nivo varnosti dostopa do storitev ali aplikacij,
- omrežje zNET ima možnost VPN dostopa za administratorje gradnikov in storitev ter vzdrževanje posameznih aplikacija eZdravja,
- omrežje zNET ima evidenco komunikacijskih povezav, lokacij in opreme ter njihovih medsebojnih relacij,
- omrežje zNET ima okolje za VPN dostope z uporabo sredstev overjanja z enkratnim geslom,
- omrežje zNET ima sistem elektronske pošte, ki omogoča razreševanje in pošiljanje elektronskih sporočil zunaj in znotraj omrežja zNET,
- omrežje zNET ima lastno CA agencijo, ki služi izdajanju certifikatov za šifriranje povezav med končnimi lokacijami in centralno lokacijo na uporabljeni komunikacijski opremi,
- omrežje zNET za oddaljene lokacije, ki se povezujejo v jedro zNET omrežje, uporablja tehnologijo SDWAN,
- omrežje zNET za upravljanje dostopa do omrežja uporablja tehnologijo Cisco ISE.

2.2 Gradniki interoperabilne hrbtenice in računalniškega omrežja

Informacijsko rešitev, ki se stoji iz interoperabilne hrbtenice in računalniškega omrežja, sestavlja kompleksno okolje, ki ga je potrebno redno vzdrževati in zagotavljati podporo proizvajalcev opreme.

V nadaljevanju se nahaja osnovni seznam strojne in programske opreme, podrobnosti o modelih, serijskih številkah, nivojih podpore posameznega proizvajalca pa se nahajajo v zaupnem/zaprtem delu Tehničnih specifikacij, ki jih bo naročnik zainteresiranim ponudnikom poslal na zahtevo ob predložitvi podpisane izjave "P-10: Izjava o varovanju zaupne dokumentacije / Potrdilo naročnika".

N	Naziv opreme	Dodaten opis	Tip opreme (HW / SW)
1.)	VMware licenčna programska oprema	Naročnina na programsko opremo VMware	SW
2.)	Strežniška ohišja	Različni proizvajalci	HW
3.)	Strežniške rezine	Strežniške rezine Dell in HPE	HW
4.)	Samostojni strežniki	Strežniki Dell in HPE	HW
5.)	Strojna oprema za shranjevanje in arhiviranje	Strojna oprema za shranjevanje in arhiviranje IBM in HPE	HW
6.)	Programska oprema za arhiviranje	Micro Focus Data Protector	SW
7.)	Sistemska programska oprema proizvajalca Microsoft	SA za Microsoft Exchange Server in Microsoft SQL Server	SW
8.)	Sistemska programska oprema proizvajalca IBM	IBM Storage Scale Data Management Edition	SW
9.)	Sistemska programska oprema proizvajalca Oracle Linux	Oracle Linux Premier Plus podpora	SW
10.)	Programska oprema za nadzor virtualne infrastrukture	Veeam Management Pack for SCOM - VMware	SW
11.)	Programska oprema za upravljanje spletnih vsebin	WordPress - postavitve v visoki razpoložljivosti	SW
12.)	Programska oprema za nadzor podatkovne baze	Solarwinds Log&Evnt Manager LEM30 NiCE OracleManagement Pack	SW
13.)	Programska oprema za varovanje pred virusi in neželeno pošto, zaščito podatkov zagotavljanje spletne varnosti.	Antivirus licenca z vzdrževanjem (s podporo proizvajalca)	SW
14.)	Delilniki bremena	Delilnik bremena Citrix Netscaler	HW
15.)	Programska oprema Red Hat	Programska oprema Red Hat	SW
16.)	Mrežna oprema	Mrežna oprema proizvajalca Cisco	HW in SW
17.)	Mrežna oprema SDWAN	Mrežna oprema SDWAN proizvajalca Cisco	HW in SW
18.)	Požarne pregrade	Požarne pregrade proizvajalca CheckPoint	HW in SW
19.)	Programska oprema za nadzor delovanja servisov	CheckMK Enterprise	SW
20.)	Orodje za upravljanje ranljivosti	Tenable sc. programska oprema	SW
21.)	SIEM programska oprema	Programska oprema IBM QRadar za varnostno zbiranje, korelacijo in analizo dogodkov	SW
22.)	Programska oprema za varovanje elektronske pošte	Clearswift	SW
23.)	Oprema za oddaljen dostop	Programska oprema za delovanje VPN dostopa	SW
24.)	Oprema za zagotavljanje varnostnih storitev	Programska in strojna oprema za upravljanje in zagotavljanje varnostnih sistemov v omrežju	SW
25.)	Programska in strojna oprema za zagotavljanje delovanja omrežja	Programska in strojna oprema za upravljanje in zagotavljanje pomožnih servisov za delovanje omrežja	SW

26.)	Programska oprema EVIDENCA	Programska oprema EVIDENCA (rešitev, ki je bila razvita za naročnika in ne vsebuje licence)	SW
27.)	Ostala podporna programska oprema	Ostala podporna programska oprema (manjši obseg)	SW

Osnovni seznam strojne in programske opreme

Razporeditev strojne opreme med lokacijama in dodatne informacije o strežniški in mrežni opremi se nahajajo v zaupnem/zaprtem delu Tehničnih specifikacij (Priloga 2).

Izvajalec mora zagotavljati pripravo in ustrezno delovanje mrežne opreme in strežniških sistemov (fizičnih in/ali virtualnih), ki delujejo na platformi, ki jo ima v lasti naročnik.

Strežniška infrastruktura zajema:

- fizični strežniki (strežniki, strežniške rezine z ohišji, strežniki za infrastrukturo vsebnikov/kontejnerjev),
- virtualni strežniki na virtualni infrastrukturi (strežniške rezine z ohišji),
- diskovne kapacitete na strežniških sistemih (fizičnih ali virtualnih) s pomočjo diskovnega podsistema.

Izvajalec bo moral v dogovoru z naročnikom ostalim ponudnikom rešitev za eZdravje omogočiti uporabo mrežne opreme, strežniške infrastrukture ali centralne baze podatkov (npr. za pripravo centralnih šifrantov, posameznih aplikacij znotraj eZdravja, ...).

2.3 Obseg projekta

Obseg projekta zajema tekoče vzdrževanje (osnovno in dopolnilno) ter upravljanje informacijske rešitve, ki ga delimo na:

- Vzdrževanje ravni informacijske rešitve (ohranjanje delujočega stanja) – osnovno vzdrževanje
 - o Preventivno vzdrževanje (nadzor rešitve, patch-anje,...);
 - o Redno administriranje uporabnikov (dodajanje posameznih IZD-jev, dodajanje uporabnikov, odvzemanje, spreminjanje pravic, ...);
 - o Vzdrževanje vseh nadgradenj;
 - o Reševanje incidentov;
- Izvajanje storitev operativnega centra kibernetkega varovanja (SOC);
- Zagotavljanje licenčne podpore za gradnike infrastrukture eZdravja;
- Izvajanje nadgradenj interoperabilne hrbtenice in računalniškega omrežja zNET;
- Upravljanje informacijske rešitve
 - o Nadzor izvajanja IT storitev;
 - o Vodenje evidenc in poročanje;
- Zagotavljanje kontaktnega centra in koordinacija reševanja zahtevkov, vključno s pomočjo pomočjo uporabnikom pri reševanju večjih težav, ki jih prvi (1) nivo podpore ne more rešiti in so povezani z uporabo systemske infrastrukture;
- Nadzor nad delovanjem informacijske rešitve in zagotavljanje SLA;
- Izvajanje dopolnilnega vzdrževanja;
- Zagotavljanje potrošnega materiala in izvajanje ostalih storitev, skladno z zahtevami v poglavju »3 – Predmet javnega naročila«.

Podroben opis obsega projekta se nahaja v nadaljevanju.

3 Predmet javnega naročila

Predmet javnega naročila je osnovno in dopolnilno vzdrževanje strojne in systemske programske opreme, potrebne za delovanje infrastrukture eZdravja in omrežja zNET, sukcesivna dobava manjše opreme in nadomestnih delov, vezanih na opremo, ki je predmet vzdrževanja, ter izvedba ostalih spremljajočih storitev, skladno z zahtevami v nadaljevanju.

Seznam strojne in programske opreme, podrobnosti o modelih, serijskih številkah, nivojih podpore proizvajalca ... se nahajajo v zaupnem/zaprtem delu Tehničnih specifikacij (Priloga 2). Ponudnik mora za vso opremo iz Priloge št. 2 zagotavljati uradno proizvajalčevo podporo za celotno obdobje trajanja tega javnega naročila (veljavnosti pogodbe).

3.1 Osnovno vzdrževanje

Namen osnovnega vzdrževanja je ohranjati optimalno delujoče stanje informacijske rešitve.

Osnovno vzdrževanje predstavlja operativno vzdrževanje in zajema:

- zagotavljanje razpoložljivosti in zahtevane odzivnosti ter kakovosti izvajanja storitev vzdrževanja strojne in systemske programske opreme,
- zagotavljanje pravilnega delovanja strojne in systemske programske opreme,
- zagotavljanje razpoložljivosti in zahtevane odzivnosti ter kakovosti izvajanja storitev vzdrževanja aplikativne programske opreme (podatkovne baze, nadzor in spremljanje delovanja naprav),
- zagotavljanje pravilnega delovanja aplikativne programske opreme (podatkovne baze, nadzor in spremljanje delovanja naprav),
- preventivno vzdrževanje,
- izvajanje postopkov posodobitve vse programske opreme in komponent sistema, ki so potrebni za pravilno in varno delovanje,
- izvajanje postopkov posodobitev in nastavitve opreme za nemoteno delovanje obstoječih sistemskih storitev,
- dvakrat letno preverjanje gradnikov visoke razpoložljivosti in redundantnih komponent sistema eZdravje,
- nujni posegi za delovanje systemske strojne in programske opreme za interoperabilno hrbtenico in računalniško omrežje zNET,
- nastavitve manjšega obsega za ureditev mrežnega prometa na centralnih in končnih točkah zNET omrežja (DNS zapisi, odpiranje vrat, usmerjanje prometa),
- postopki izdelave in zagotavljanje varnostne kopije podatkov in replikacije podatkov na nivoju diskovnega podsistema ter vzpostavitev ponovnega stanja delovanja pred vzrok za vrnitev v ponovno stanje delovanja (vzrok za uporabo varnostne kopije podatkov),
- vzdrževanje nastavljenih elementov rešitev, kot so šifranti, registri, enolični krajevnik virov (URL-ji), ...,
- analiza možnih izboljšav ali optimizacij rešitev ter izdelava predlogov za optimizacijo za naročnika,
- upravljanje virtualnih strežnikov, upravljanje s sistemom data center recovery na nivoju virtualizacije za sisteme VMware in OLVM,
- upravljanje in vzdrževanje kontejnerske platforme Kubernetes v obstoječem okolju Red Hat OpenShift,

- redno administriranje uporabnikov (dodajanje, odvzemanje, spreminjanje pravic, ...), nudenje strežniške infrastrukture in CBP na sistemskem nivoju za potrebe drugih aplikacij,
- upravljanje fizičnega in logičnega nivoja omrežja zNET,
- upravljanje in zagotavljanje delovanja varnega sistema oddaljenega dostopa do omrežja (VPN koncentratorji),
- upravljanje in zagotavljanje delovanja varnostnih sistemov v omrežju (požarne pregrade) in sistemi za odkrivanje in preprečevanje vdorov,
- upravljanje in zagotavljanje pomožnih servisov za delovanje omrežja (DNS, PROXY, NTP, CA, Monitoring, ...),
- reševanje napak pri delovanju v okviru predvidenega odzivnega časa,
- priprava ponudb za dopolnilno vzdrževanje, pomoč uporabnikom (drugi in tretji nivo podpore),
- odkrivanje in odpravljanje skritih napak in pomanjkljivosti v kodi aplikativne programske opreme,
- spremljanje tehnoloških novosti, povezanih z vzdrževano programsko opremo ter priprava predlogov in ukrepov za nemoteno delovanje oz. izboljšanje njenega delovanja,
- objava novih verzij in novonastale dokumentacije, ki so posledica odprave napak in pomanjkljivosti, v repozitoriju naročnika in distribucija programerskim hišam,
- reševanje problemov ter predlaganje ukrepov za nemoteno delovanje aplikativne programske opreme in optimizacijo delovanja,
- preverjanje delovanja aplikacije na različnih okoljih, ažurno vzdrževanje dokumentacije sistema,
- redno preverjanje pravilnosti in optimalnosti delovanja sistema,
- intervencije v primeru anomalij, ki jih zazna sam ali jih sporoči naročnik oz. uporabniki,
- učinkovito pomoč in svetovanje ključnim uporabnikom na strani naročnika,
- redno spremljanje delovanja rešitev in poročanje naročniku,
- izdelava rednih in izrednih poročil o delovanju rešitve, ki je predmet vzdrževanja,
- upravljanje in vzdrževanje podatkovnih baz Microsoft SQL Server (administracija, nadzor delovanja, posodobitve in varnostni popravki ter optimizacija zmogljivosti),
- upravljanje in vzdrževanje podatkovnih baz Oracle Database (administracija, nadzor delovanja, posodobitve in varnostni popravki ter optimizacija zmogljivosti),
- upravljanje in vzdrževanje sistema Oracle Exadata Database Machine (Engineered System) – spremljanje delovanja, konfiguracija, nameščanje posodobitev ter optimizacija zmogljivosti podatkovnega okolja,
- upravljanje in vzdrževanje naprave za varnostno kopiranje Oracle Zero Data Loss Recovery Appliance (ZDLRA) – konfiguracija in nadzor varnostnega kopiranja ter obnovitve podatkovnih baz, spremljanje replikacije in razpoložljivosti.
- nadzor sistema:
 - o spremljanje in zbiranje dogodkov iz sistema;
 - o periodično pregledovanje delovanja podatkovne zbirke;
 - o stalno spremljanje delovanja podatkovnih virov integriranih na nivoju celotne interoperabilne hrbtnice eZdravja in ukrepanje v primeru morebitnih motenj;
 - o tehnično usklajevanje s posameznimi podatkovnimi viri za zagotovitev operativnega delovanja;
 - o predlogi ukrepov za preventivno reševanje;
- upravljanje razpoložljivosti, zmogljivosti in kapacitete sistema:
 - o spremljanje stanja in trendov sistema;
 - o identificiranje kazalnikov oz. pokazateljev, preko katerih spremljamo, da obratovanje ni ogroženo;

- priprava predlogov in izvajanje ukrepov za zagotovitev zahtevane razpoložljivosti, zmogljivosti (optimizacija) in kapacitete;
- koordinacija izvedbe ukrepov (obveščanje pristojnih oseb), posredovanje dogodka v izvajanje ustreznim izvajalcem;

Zraven splošnih zahtev za osnovno vzdrževanje, ki veljajo za vse tehnologije in storitve, ki so predmet vzdrževanja, je potrebno v okviru vzdrževanja upoštevati tudi posebne zahteve za posamezne tehnološke rešitve. Zahteve so opredeljene v nadaljevanju.

3.1.1 Vzdrževanje opreme proizvajalca Cisco

V okviru vzdrževanja standardne omrežne opreme proizvajalca Cisco Systems, Inc., se mora zagotoviti:

- zamenjava okvarjene opreme naslednji delovni dan,
- sprejem prijave okvare in odprava okvare na okvarjeni opremi v dogovorjenem režimu, ki vključuje tudi menjavo strojne opreme glede na režim vzdrževanja (glej poglavje »Odzivni časi in zagotavljanje SLA«),
- zagotavljanje vseh izdanih programskih popravkov in obveščanje naročnika o novih verzijah in spremembah v njih (angl.: Patch),
- zagotavljanje vseh izdaj programske opreme in strojne programske opreme (angl.: Minor and Major Software Releases) v sklopu iste funkcionalnosti,
- dostop do tehnoloških informacij proizvajalca opreme v času veljavnosti pogodbe,
- obveščanje naročnika o varnostnih problemih z obstoječimi verzijami programske opreme in takojšnja izvedba akcij v dogovoru z naročnikom, če obstaja varnostna ogroženost na opremi, ki jo ima naročnik, ter
- vodenje dokumentacije vzdrževalnih posegov na opremi naročnika
 - Naročnik mora imeti možnost vpogleda v dokumentacijo (preko interneta) za čas trajanja te pogodbe.

Naročnik lahko prijavi okvaro v režimu 24/7/365. Naročnik lahko prijavi okvaro na podlagi pisne prijave, elektronske prijave, lahko tudi telefonsko, izven rednega delovnega časa izvajalca pa mu je na voljo številka mobilnega telefona dežurnega vzdrževalca.

V primeru nepravilnega delovanja programske opreme, izvajalec naročniku nudi tehnično pomoč, obvesti proizvajalčev center za tehnično pomoč (TAC) o zaznani napaki. Takoj, ko proizvajalec dobavi novo različico programske opreme, izvajalec v dogovoru z naročnikom, izvede namestitev nove programske opreme.

Storitev mora vključevati vse potrebne nadomestne dele, material, potne stroške in delo potrebno za odpravo okvare v omrežju.

V okviru vzdrževanja opreme Cisco SDWAN mora Izvajalec izvajati aktivnosti, ki so opredeljene v nadaljevanju.

Storitve vzdrževanja za Core SDWAN (Centralni sistem):

- vzdrževanje, nadgradnje in varnostne kopije centralnih krmilnih komponent (vManage, vSmart, vBond),
- upravljanje globalnih usmerjevalnih politik in sistemske topologije,

- skrb za digitalna potrdila (certifikate) in licenčnine za celoten sistem, in
- integracija krovnega sistema z drugimi rešitvami naročnika (nadzor, SIEM).

Storitve vzdrževanja za EndPoint SDWAN (Oddaljene lokacije)

- fizična namestitvev, vzdrževanje in zamenjava strojne opreme (usmerjevalnikov) na lokacijah,
- konfiguracija in upravljanje lokalnih omrežnih priklopov (LAN/WAN) ter lokalnih varnostnih in QoS politik,
- posodabljanje programske opreme na samih robnih usmerjevalnikih, in
- odpravljanje napak ob izpadih in direktna komunikacija z lokalnimi internetnimi ponudniki (ISP).

3.1.2 Vzdrževanje opreme proizvajalca Check Point

V okviru vzdrževanja opreme proizvajalca Check Point, se mora izvajati:

- sprejem prijave okvare in odprava okvare na okvarjeni opremi v dogovorjenem režimu, ki vključuje tudi menjavo strojne opreme glede na režim vzdrževanja,
- zagotavljanje vseh izdanih programskih popravkov in obveščanje naročnika o novih verzijah in spremembah v njih (angl.: Patch),
- zagotavljanje vseh izdaj programske opreme in strojne programske opreme (angl.: Minor and Major Software Releases) v sklopu iste funkcionalnosti,
- dostop do tehnoloških informacij proizvajalca opreme v času veljavnosti pogodbe,
- obveščanje naročnika o varnostnih problemih z obstoječimi verzijami programske opreme in takojšnja izvedba akcij v dogovoru z naročnikom, če obstaja varnostna ogroženost na opremi, ki jo ima naročnik,
- vodenje dokumentacije vzdrževalnih posegov na opremi naročnika
 - o Naročnik mora imeti možnost vpogleda v dokumentacijo (preko interneta) za čas trajanja te pogodbe.

Storitev mora vključevati vse potrebne nadomestne dele, material, potne stroške in delo potrebno za odpravo okvare v omrežju.

3.1.3 Upravljanje kontejnerskega okolja Red Hat OpenShift

Izvajalec zagotavlja upravljanje, vzdrževanje in podporo za platformo Red Hat OpenShift, kar vključuje:

- upravljanje uporabniških računov, vlog in dostopnih pravic,
- nameščanje, konfiguracijo in vzdrževanje OpenShift operaterjev (Operators),
- izvajanje rednih posodobitev, varnostnih popravkov in nadgradenj platforme,
- upravljanje in konfiguracijo sistemov za beleženje dogodkov (logging) ter spremljanje delovanja (monitoring),
- spremljanje stanja in razpoložljivosti platforme,
- podporo pri nameščanju, konfiguraciji in upravljanju aplikacij v okolju OpenShift,
- prvo raven podpore za aplikacije, nameščene v okolju Kubernetes/OpenShift,

- analizo incidentov, odpravljanje napak ter pripravo predlogov za izboljšave in optimizacijo delovanja okolja,
- konfiguracijo in upravljanje Citrix okolja za podporo aplikacijam, ki delujejo v povezavi z OpenShift platformo,
 - o odpravljanje težav in optimizacijo integracije med Citrix in OpenShift okoljem,
 - o podporo pri spremembah konfiguracij in nadgradnjah sistema Citrix,
- upravljanje, vzdrževanje in nadgradnje GitLab okolja,
 - o nameščanje varnostnih popravkov,
 - o podporo uporabnikom pri uporabi GitLab funkcionalnosti,
 - o svetovanje glede uporabe dobrih praks pri upravljanju izvirne kode, repozitorijev in CI/CD procesov.

Ker ima naročnik trenutno še v uporabi tudi okolje OKD, se smiselno enako kot za okolje OpenShift, zahtevane storitve za OpenShift izvajajo tudi za okolje OKD.

3.1.4 Upravljanje virtualizacijskega okolja Linux in OLVM

Izvajalec zagotavlja upravljanje, vzdrževanje in podporo za virtualizacijsko platformo Linux, kar vključuje:

- pripravo in vzdrževanje standardiziranih predlog (templates) skladno s CIS varnostnimi priporočili,
- vzpostavitev novih virtualnih strežnikov,
- upravljanje uporabniških računov in dostopnih pravic,
- izvajanje nadgradenj operacijskega sistema in nameščanje varnostnih popravkov,
- spremljanje delovanja strežnikov in odpravljanje incidentov,
- upravljanje strojnih virov virtualnih strežnikov (CPU, pomnilnik, diskovni prostor),
- dodajanje in razširjanje diskovnih kapacitet,
- avtomatizacijo administrativnih postopkov in upravljanja strežniškega okolja,
- namestitve, konfiguracijo in vzdrževanja sistema Uyuni za upravljanje popravkov,
- upravljanje in vzdrževanje Oracle Linux Virtualization Manager (OLVM) okolja:
 - o izvajanje sistemskih posodobitev in nadgradenj,
 - o upravljanje virtualnih strežnikov in virtualizacijske infrastrukture,
 - o konfiguracijo in upravljanje virtualnih omrežij,
 - o spremljanje delovanja okolja ter odpravljanje incidentov.

3.1.5 Upravljanje sistemov IBM Storage Scale in Hashicorp Vault

Izvajalec zagotavlja upravljanje in vzdrževanje IBM Storage Scale, kar vključuje:

- izvajanje nadgradenj operacijskega sistema in komponent IBM Storage Scale,
- nameščanje varnostnih popravkov,
- konfiguracijo in upravljanje datotečnih sistemov, filesetov, kvot in diskovnih kapacitet,
- spremljanje delovanja, zmožljivosti, razpoložljivosti in zasedenosti sistema,
- upravljanje visoke razpoložljivosti ter podporo pri obnovi po izpadu,
- odpravljanje napak, incidentov in težav z zmožljivostjo,
- podporo uporabnikom in aplikativnim ekipam.

Izvajalec zagotavlja upravljanje in vzdrževanje IBM Hashicorp Vault, kar vključuje:

- upravljanje uporabnikov, skupin, vlog in dostopnih pravic,
- konfiguracijo in vzdrževanje avtentikacijskih metod ter varnostnih politik,
- upravljanje statičnih in dinamičnih skrivnosti,
- izvajanje nadgradenj in nameščanje varnostnih popravkov,
- spremljanje delovanja, razpoložljivosti,
- odpravljanje napak in varnostnih incidentov,
- podpora uporabnikom ter aplikativnim ekipam.

3.1.6 Upravljanje podatkovnih baz na strojni opremi Exadata X11M Compute

Izvajalec zagotavlja upravljanje in vzdrževanje Exadata X11M Compute, kar vključuje:

- administracija in vzdrževanje podatkovnih baz Oracle na platformi Exadata,
- spremljanje zmogljivosti sistema in optimizacija delovanja podatkovnih baz,
- izvajanje varnostnih kopij (RMAN) ter postopkov obnovitve podatkov,
- nameščanje popravkov in nadgradenj Oracle baz,
- upravljanje visoke razpoložljivosti z Oracle RAC in Data Guard,
- analiza in odpravljanje napak ter reševanje incidentov v produkcijskem okolju,
- spremljanje porabe virov ter načrtovanje kapacitet sistema,
- avtomatizacija administrativnih opravil s skriptami (Shell, SQL, PL/SQL),
- sodelovanje pri migracijah podatkovnih baz in implementaciji novih rešitev.

3.2 Dopolnilno vzdrževanje

Dopolnilno vzdrževanje, oziroma nadgradnja informacijske rešitve, se v dogovoru z naročnikom izvaja v primeru:

- naknadno definiranih dopolnitev glede na spremembe v uporabniških zahtevah,
- povezave oz. morebitne integracije z različnimi informacijskimi sistemi,
- dodatnih potreb naročnika, ki bi se pokazale med uporabo rešitve.

3.2.1 Dopolnilno vzdrževanje predvidoma zajema:

- sodelovanje pri analizi in pripravi specifikacij uporabniških zahtev za dodajanje novih in izboljšanje obstoječih funkcionalnosti programske opreme,
- dopolnitve komponent rešitev zaradi nadgradnje obstoječih ali vključevanja novih rešitev,
- dopolnitve komponent rešitev zaradi optimizacije delovanja,
- dopolnitev dokumentacije rešitev po izvedenih dopolnitvah,
- izboljšanje obstoječih funkcionalnosti programske opreme,
- izboljševanje lastnosti delovanja, uporabnosti in dograjevanje novih funkcionalnosti ter modulov na podlagi predlogov naročnika, uporabnika ali izvajalca in s strani naročnika potrjenih specifikacij,
- prilagajanje programske opreme glede na spremembe systemskega okolja in operacijskega sistema v okviru možnosti in zagotovil proizvajalcev oziroma principalov ter glede na potrebe ostalih povezanih informacijskih sistemov,
- prilagajanje in dograjevanje programske opreme glede na vsebinske spremembe,
- nastavitve usmerjevalnikov za priklop obstoječih in novih centralnih točk / končnih lokacij v zNET omrežju,
- priprava analitičnih izdelkov (poročila, statistike),

- odlaganje novih verzij, ki so posledica dopolnilnega vzdrževanja, v repozitorij naročnika in distribucija programerskim hišam,
- dokumentiranje novih verzij in funkcionalnosti, ki so rezultat dopolnilnega vzdrževanja,
- dopolnilno vzdrževanje za SDWAN, SIEM in SOC, kot je opredeljeno v nadaljevanju.

3.2.2 Dopolnilno vzdrževanje SDWAN zajema:

- spremembe nastavitve obstoječih in priklop novih usmerjevalnikov v zNET omrežju (menjava ponudnika MPLS), ob prekoračitvi števila posegov v osnovnem vzdrževanju:
 - o ocena: 200 priklopov;
- spremembe nastavitve obstoječih in priklop novih usmerjevalnikov v zNET omrežju za priklop zasebnikov zdravstvene dejavnosti s storitvijo ponudnikov najetih povezav z opremo, ob prekoračitvi števila posegov v osnovnem vzdrževanju:
 - o ocena: 1500 priklopov;
- priklop lastnega internetnega segmenta,
- vzpostavitev testnega okolja za priklop zasebnikov zdravstvene dejavnosti s storitvijo ponudnikov najetih povezav z opremo,
- certificiranje opreme za priklop v zNET omrežje,
- razširjanje funkcionalnosti informacijske rešitve, vključno z dopolnjevanjem, spreminjanjem ali dograjevanjem informacijske rešitve sporazumno z naročnikom; prilagajanje informacijske rešitve glede na spremembe okolja licenčnega programja, v katerem deluje informacijska rešitev sporazumno z naročnikom,

3.2.3 Dopolnilno vzdrževanje SIEM zajema:

- dodajanje novih primerov uporabe (use cases),
- dodajanje in konfiguracija novih aplikacij (UBA, DNS,...).
- izdelava zahtevnejših poizvedb,
- izdelava zahtevnejših poročil,
- urejanje in optimiziranje kompleksnih varnostnih pravil,
- optimizacija modula za spremljanje in pregledovanja omrežnega prometa, in
- prenos znanja o novostih pri programski opremi.

3.2.4 Dopolnilno vzdrževanje v okviru zagotavljanja odzivne skupine CSIRT:

- Odzivna skupina - CSIRT (Cyber Security Incident Response Team) za potrebe vodenja procesa odprave kibernetске grožnje na lokaciji naročnika, poznavanje procesa zavarovanja forenzičnih dokazov za kasnejšo obdelavo, skladno s slovensko zakonodajo.
- Odzivna skupina - CSIRT (Cyber Security Incident Response Team) skupina mora biti naročniku na voljo na zahtevo. Sestavljati jo morajo vrhunski strokovnjaki s področij kibernetškega varovanja, vrednotenja tveganj informacijskega varovanja in specialisti področij: omrežnih tehnologij, požarnih pregrad naslednjih generacij), ter po potrebi tehnološki specialisti. Odzivna skupina mora obsegat najmanj 4 tehnološke specialiste, ki so vključeni v aktivnosti reševanje kibernetških incidentov.
- Primarna naloga odzivne skupine je sodelovanje z naročnikom in njegovimi strokovnimi ekipami (vključno s strokovnimi ekipami izvajalcev tehnološkega upravljanja IKT virov), vodenje procesa odprave kibernetске grožnje na lokaciji naročnika, poznavanje procesa zavarovanja forenzičnih

dokazov za kasnejšo obdelavo skladno z ustaljenimi postopki. Naloge odzivne skupine na področju reševanja varnostnega / kibernetkega incidenta predstavljajo predvsem:

- Priprava
 - o Priprava na reševanje incidentov;
 - o Preprečevanje incidentov (proaktivne naloge in sodelovanje z Ravnjo-1 in Ravnjo-2);
- Zaznavanje in analiza
 - o vektorjev napada;
 - o prepoznavanje dodatnih znakov varnostnega incidenta;
 - o viri predhodnikov in kazalnikov;
 - o analiza incidentov;
 - o dokumentacija o incidentu;
 - o prioritizacija incidentov;
 - o obveščanje o incidentu.
- Zadrževanje, izkoreninjenje grožnje in obnovitev
 - o izbira strategije za zatiranje;
 - o zbiranje dokazov in ravnanje z njimi;
 - o prepoznavanje gostiteljskih napadalcev;
 - o izkoreninjenje in obnovitev.
- Aktivnosti po incidentu
 - o analiza in dopolnjevanje pravil;
 - o uporaba zbranih podatkov o incidentu;
 - o pridrževanje dokazov.
- Kontrolni seznam za ravnanje z varnostnimi incidenti
- Priporočila

3.2.5 Ostale storitve dopolnilnega vzdrževanja

- V dopolnilno vzdrževanje se lahko vključi tudi ostale dodatne storitve skladno z izkazanimi zahtevami.

3.3 Storitve operativnega centra kibernetkega varovanja

Storitve operativnega centra kibernetkega varovanja se sestoji iz:

- vzdrževanja sistema SIEM, in
- izvajanje storitev varnostno operativnega centra - SOC.

3.3.1 Vzdrževanje sistema SIEM

Vzdrževanje operativne ravni delovanja Sistema SIEM zajema:

- optimizacija delovanja vzdrževanega okolja,
- nadgradnje programske opreme SIEM in operacijskega sistema po priporočilih proizvajalca,
- reševanje sistemskih incidentov in problemov,
- spremljanje delovanja in posredovanje na daljavo,
- telefonska pomoč pri opravih na vzdrževanem sistemu,
- redni mesečni pregledi sistema z ugotovitvami in predlogi za izboljšave,

- koordinacija del s principalom pri morebitnem odpravljanju napak na vzdrževani opremi (PMR),
- izvajanje zahtevkov po spremembah (npr. odprava false positive alarmov, fine tuning vhodnih podatkov, dodajanje novih virov, ...),
- urejanje in optimiziranje osnovnih varnostnih pravil,
- nastavljanje obveščanja za željene tipe incidentov, in
- uvedba novih funkcionalnosti in pomoč pri implementaciji novih virov (log sources).

3.3.2 Izvajanje storitev varnostno operativnega centra - SOC

Storitev varnostno operativnega centra – SOC se izvaja na dveh ravneh:

- SOC raven – 1: Postopek triažiranja
- SOC raven – 2: Upravljanje varnostnih dogodkov

V postopku triažiranja (SOC raven – 1) se na osnovi dodatno zbranih informacij o varnostnem prestopku določiti izvor, cilj in vpliv varnostnega prestopka, opredeli stopnjo ranljivosti ter pripraviti načrt reševanja varnostnega prestopka glede.

Po končanem postopku triažiranja sledi upravljanje z varnostnim dogodkom (SOC raven – 2), obseg aktivnosti na SOC ravni – 1 in SOC ravni – 2 pa je opredeljen v nadaljevanju.

SOC raven-1: Postopek triažiranja

SOC Raven-1 zagotavlja pregled vseh varnostnih dogodkov in identifikacijo tistih, ki potrebujejo podrobnejšo raziskavo. SOC Raven-1 zajema:

- triažiranje, katerega osnovni namen je na osnovi dodatno zbranih informacij o varnostnem prestopku določiti izvor, cilj in vpliv varnostnega prestopka, potrditi ali dopolniti sistemsko določeno stopnjo ranljivosti, pripraviti predlog in načrt reševanja ter prioritizacijo odgovora na varnostni dogodek,
- neprekinjeno spremljanje varnostnih dogodkov, prepoznanih preko SIEM, spremljanje in analiza omrežnega prometa, naprav, gradnikov in aplikacij,
- začetna klasifikacija in označevanje vsakega novega varnostnega dogodka,
- takojšnje ukrepanje - triaža varnostnega dogodka, skladno z uvedeno kategorizacijo (prioriteta in resnost) in veljavnimi operativnimi navodili,
- določitev stopnje kritičnosti (eskalacija) prednostnih dogodkov ustrezni ekipi,
- sodelovanje s storitvenim središčem, evidentiranje in upravljanje varnostnih dogodkov v TTS sistemu ter v sistemu naročnika,
- sodelovanje z drugimi deležniki v konzorciju pri razreševanju varnostnih dogodkov, ter
- vodenje in koordinacija razreševanja varnostnih incidentov.

Po končani stopnji triažiranja, se varnostne dogodke, ki potrebujejo nadaljnjo obravnavo, prevzame v upravljanje (SOC raven-2), kjer je potrebno zagotavljati vire in izvajati aktivnosti, ki so opredeljene v nadaljevanju.

SOC raven – 2: Upravljanje varnostnih dogodkov

Vodenje operativne izvedbe:

Ponudnik mora zagotoviti strokovnjaka (kot na primer: Security TAM – technical account manager) za operativno vodenje razreševanja varnostnih operacij, katerega naloge so:

- poročanje o potencialnih varnostnih tveganjih,
- sodelovanje pri pripravi predlogov za zmanjšanje kibernetских tveganj,
- proaktivno obveščanje o varnostnih tveganjih,
- eskalacije in spremljanje izvedbe,
- primarni kontakt za vprašanja povezana z informacijsko varnostjo zNET omrežja,
- vodenje, organiziranje, usklajevanje in nadzor izvedbe,
- priprava strokovnih podlag s področja dela,
- priprava navodil in scenarijev za ukrepanje v posebnih primerih,
- zbiranje, preučevanje in posredovanje idej, predlogov in izboljšav s strani področja varnosti,
- nadzorovanje učinkovitosti in odgovornost za pravilnost poteka procesa,
- pripravljanje podatkov in izdelovanje izrednih poročil,
- izdelovanje in posredovanje poročil za vodstvo oziroma varnostni kolegij,
- obveščanje skrbnikov informacijskih virov za pregled in izdelavo poročil za oceno tveganja,
- hierarhična eskalacija ob zastoju procesa.

3.4 Zagotavljanje kontaktnega centra in koordinacija reševanja zahtevkov

Kot je navedeno že v poglavju 2, je predmet javnega naročila tudi pomoč uporabnikom pri reševanju večjih težav na drugem (2) nivoju, ki jih prvi (1) nivo podpore ne more rešiti in so povezani z uporabo sistemske infrastrukture.

V ta namen mora ponudnik zagotavljati Kontaktni center - KC (ang. Servicedesk - SD), ki predstavlja osrednjo kontaktno točko, preko katere poteka vsa operativna, tehnična in administrativna komunikacija ter kjer se sprejemajo in evidentirajo vsi zahtevki, incidenti in spremembe pri izvajanju IT storitev.

Tehnične zahteve za kontaktni center - KC:

- delovni čas klicnega centra 24/7/365 (24 ur dnevno, vse dni v letu),
- 90% klicev odgovorjenih v roku 30 sekund,
- vsaj 10 ITIL lastnih certificiranih svetovalcev*,
- vzpostavljen sistem za spremljanje in vodenje incidentov,
- vodja KC mora imeti pridobljen enega izmed certifikatov ITIL 4 Master ali HDI Support center director.

* OPOMBA: Naročnik si pridržuje pravico, da od ponudnika kadarkoli med izvajanjem pogodbe zahteva predložitev dokazil o usposobljenosti (pridobljenimi certifikati ITIL) s strani svetovalcev. Izpolnjevanje te zahteve ni pogoj za sodelovanje, ki bi se preverjal v fazi ocenjevanja ponudb, temveč pogodbeni obveznost izvajalca ves čas trajanja pogodbe.

Naloge KC zajemajo:

- sprejem, evidentiranje eskaliranje ter razvrščanje incidentov v skladu z SLA,

- koordinacija zahtevkov znotraj konzorcija in z zunanjimi izvajalci,
- obveščanje / najava posegov znotraj in zunaj konzorcija,
- vodenje zgodovine obravnav (mail ali snemanje klicev/SMS sporočila),
- obveščanje naročnika o stanju zahtevkov,
- vodenje in koordinacija razreševanja varnostnih incidentov v sodelovanju s SOC,
- pravočasno obveščanje naročnika ob preseganju SLA na incidentih,
- nadzorni pregled nad odprtimi incidenti, zahtevki ter po potrebi eskalacija, in
- sodelovanje z zunanjimi izvajalci pri iskanju možnih vzrokov za težave pri delovanju.

Zahteve za sistem za spremljanje in vodenje incidentov:

- ponudnik mora zagotoviti sistem za upravljanje ter vodenje incidentov in zahtevkov, ki mora biti na razpolago tudi naročniku,
- sistem mora biti nameščen v informacijskem sistemu eZdravja ali na infrastrukturi v Republiki Sloveniji (rešitve v oblaku izven RS niso sprejemljive),
- rešitev ne sme biti razvita posebej za naročnika, temveč mora ponudnik zagotoviti eno izmed standardnih in že uveljavljenih rešitev na trgu,
- zagotovljene morajo biti vse potrebne licence za uporabo, tako za spletni dostop, kot za dostop preko mobilne aplikacije,
- ponudnik mora skrbeti, da je dokumentacija posameznih zahtevkov urejena, kar pomeni, da morajo biti odstranjena vsa ne relevantna besedila in slike, kot so logotipi, pravna obvestila in podobno,
- ob prenehanju pogodbe mora izvajalec na zahtevo naročnika predati naročniku celotno zgodovino zahtevkov in bazo znanja v odprtem/izvozljivem formatu.

Ponudnik mora za potrebe reševanja incidentov in zahtevkov ves čas trajanja pogodbe zagotoviti strokovno usposobljenega SLA manager-ja, ki skrbi, da se dogovorjeni odzivni in časi rešitev ter druge SLA metrike merijo, spremljajo, poročajo in po potrebi eskalirajo (v kolikor bi prihajalo do odstopanj).

Naloge SLA manager-ja zajemajo:

- primarni eskalacijski kontakt za naročnika,
- izdelava izrednih poročil (delovanje sistema, zmogljivosti, incidenti – P1),
- koordinacija reševanja kompleksnih incidentov,
- poročanje o statusu incidentov/ zahtevkov in doseganju SLA rokov.

3.5 Izvajanje storitvenih zahtevkov, vodenje evidenc, koordinacija, poročanje in spremljanje obsega izvedenih del

Izvajalec je v okviru Osnovnega in Dopolnilnega vzdrževanja dolžan vzdrževati in upravljati naročnikovo strojno in programsko opremo skladno z določili teh Tehničnih specifikacij. Pri tem mora postopke izvajati na način, da bodo omogočali vodenje, spremljanje in nadzor evidenc prijav napak, varnostnih incidentov, zahtevkov za administracijo uporabnikov, ipd. ter posledično omogočali pripravo verodostojnih poročil.

Izvajalec je dolžan na dnevni ravni ažurno voditi naslednje evidence:

- evidenco incidentov,
- evidenco varnostnih incidentov,
- evidenco zahtev za administriranje uporabnikov, in
- evidenco aktivnosti na področju kibernetiko varnosti.

Pri tem je v primeru incidentov in varnostnih incidentov je na zahtevo naročnika izvajalec dolžan v najkrajšem razumnem roku pripraviti pisno ali elektronsko poročilo in ga posredovati odgovorni osebi naročnika, podrobno obliko in vsebino poročil pa bosta naročnik in izvajalec določila v fazi prevzema vzdrževanja informacijske storitve.

Vsebina poročil ter opis postopkov upravljanja in vzdrževanja se nahaja v nadaljevanju.

3.5.1 Izvajanje storitvenih zahtevkov

Izvajalec je v okviru osnovnega in dopolnilnega vzdrževanja dolžan izvajati nadgradnje in druge vsebinske in tehnične zahteve naročnika.

Podroben opis procesov nalog / vzdrževanja omrežja zNET je opisan v »Prilogi 1: Storitve vzdrževanja in upravljanja omrežja zNET«, pred izvajanjem storitvenih zahtevkov, pa mora izvajalec predhodno prejeti soglasje, kot je opredeljeno v nadaljevanju.

Soglasje za izvedbo sprememb v informacijskem sistemu eZdravja

Predhodno soglasje za ne nujne spremembe

Izbrani ponudnik se zaveže, da bo za vsako ne nujno spremembo, ki jo namerava izvesti v informacijskem sistemu, pridobil predhodno pisno soglasje skrbnikov informacijsko-komunikacijske tehnologije (IKT). Ne nujne spremembe so tiste, ki ne zahtevajo takojšnje izvedbe za nemoteno delovanje informacijskega sistema ali kjer ni neposredne grožnje za integriteto, varnost ali zasebnost podatkov v sistemu.

Zahteva za soglasje mora vsebovati:

- podrobno opisano naravo in obseg predlagane spremembe,
- razloge za spremembo,
- predviden termin za izvedbo spremembe,
- morebitna tveganja in njihovo obravnavo, in
- soglasje za nujne spremembe.

Izvajanje nujnih sprememb

V primeru nujne spremembe, ki zahteva takojšnjo izvedbo zaradi zagotavljanja neprekinjenega delovanja informacijskega sistema ali varstva podatkov, izbrani ponudnik pridobi soglasje dežurnega skrbnika IKT preko telefona. Če dežurni ni dosegljiv, lahko izvede spremembo brez predhodnega soglasja, v vsakem primeru pa je dolžan o spremembi ter razlogih za njo pisno obvestiti skrbnike IKT najpozneje v roku 24 ur po izvedbi spremembe. Nujna sprememba se lahko izvaja samo v izjemnih okoliščinah, kjer je ogrožena stabilnost, varnost ali zasebnost informacijskega sistema.

Poročilo o nujni spremembi mora vključevati enake podatke kot odobritev za ne nujno spremembo ter dodatno še obrazložitev, zakaj ni bilo možno pridobiti predhodnega soglasja.

3.5.2 Vodenje evidenc in poročanje

Poročanje se izvaja na mesečnem nivoju oziroma v primeru potreb tudi na zahtevo.

Mesečna poročila za prejšnji mesec morajo biti priložena pred izstavitvijo računa. Naročnik ima 5 delovnih dni časa za podati morebitne pripombe na priložena poročila. Poročila potrjena s strani naročnika so predpogoj za izstavitvev računa.

Ponudnik mora pripraviti vsebinsko ločena poročila, kot sledi (vsebina mesečnih poročil se lahko tekom izvajanja pogodbe spreminja):

Zbirno poročilo o ugotovljenih in /ali prijavljenih incidentih:

- oznaka incidenta,
- kratek opis incidenta,
- datum in čas prijave incidenta,
- prijavitelj incidenta,
- stopnja incidenta,
- datum in čas začetka odpravljanja incidenta,
- datum in čas odprave incidenta,
- status incidenta na dan zadnji dan v mesecu, in
- kratek opis odpravljanja incidenta.

Zbirno poročilo o varnostnih incidentih:

- oznaka varnostnega incidenta,
- kratek opis varnostnega incidenta,
- datum in čas prijave varnostnega incidenta,
- prijavitelj varnostnega incidenta,
- stopnja varnostnega incidenta,
- datum in čas začetka odpravljanja varnostnega incidenta,
- datum in čas odprave varnostnega incidenta,
- vzrok varnostnega incidenta,
- ocenjena nastala škoda,
- kratek opis odpravljanja napake,
- status na dan zadnji dan v mesecu, in
- predlagani ukrepi za preprečevanje ponovitve varnostnega incidenta.

Zbirno poročilo o Administratorskih zahtevkih:

- oznaka zahtevka,
- kratek opis zahtevka,
- datum in čas zahtevka,
- prijavitelj zahtevka,

- kratek opis opravljene aktivnosti,
- status zahtevka, in
- status na dan zadnji dan v mesecu.

Zbirno poročilo o izvedenih preventivnih vzdrževalnih aktivnostih:

- datum aktivnosti, in
- kratek opis.

Mesečna poročila morajo biti pripravljena tako, da omogočajo popolno sledljivost med:

- pogodbo,
- posameznim naročilom oziroma zahtevkom,
- izvedenimi aktivnostmi,
- dokazili o izvedbi,
- prevzemnimi zapisniki (kadar se uporabljajo),
- izstavljenim računom.

Za vsako izvedeno storitev oziroma aktivnost mora biti razvidno najmanj:

- enolična oznaka aktivnosti oziroma zahtevka,
- vrsta storitve (osnovno vzdrževanje, dopolnilno vzdrževanje, odprava incidenta, administrativni poseg, preventivno vzdrževanje, projektna naloga ipd.),
- datum in čas začetka izvajanja,
- datum in čas zaključka izvajanja,
- poraba časa po osebah, ki so sodelovale pri izvedbi, po možnosti s točno opredelitvijo kdaj je bilo delo opravljeno (izjemo predstavlja izvajanje storitev s strani timov, kjer aktivnosti niso vezane na specifični kader / posameznika),
- opis izvedenih aktivnosti,
- infrastruktura oziroma sistem na katerem so bile aktivnosti izvedene (kadar je relevantno),
- rezultat izvedene aktivnosti (kot npr. ali je bila aktivnost uspešno izvedena ali ne, ali so potrebne še kakšne ostale aktivnosti, ipd.),
- dokazilo o izvedbi oziroma sklic na tehnično evidenco (ticket, dnevnik aktivnosti, sistemski log, zapisnik testiranja, konfiguracijska sprememba, zapis v CMDB ali drugo ustrezno dokazilo),
- število opravljenih ur,
- urna postavka oziroma druga pogodbeni obračunska enota, vrednost posamezne aktivnosti brez DDV (za aktivnosti v okviru dopolnilnega vzdrževanja, ki niso podrobno opredeljene v Pogodbi).
- Navedba konzorcijskega partnerja, ki je izvedel posamezno aktivnosti (velja v primeru skupne ponudbe / konzorcija).

V primeru pavšalnega vzdrževanja mora ponudnik v mesečnem poročilu izkazati vse izvedene aktivnosti, ki so bile opravljene v okviru pavšala, ne glede na to, da niso obračunane posamezno.

V primeru storitev, ki se obračunavajo po dejansko opravljenih urah ali drugi obračunski enoti, mora biti iz mesečnega poročila nedvoumno razviden izkaz opravljenih aktivnosti ter primerjava med opravljenimi in predvidenimi aktivnostmi, če je to mogoče (kot na primer pri dopolnilnem vzdrževanju). Določilo ne velja za pripravljenost in zagotavljanje SLA, izvajanje storitev NOC in SOC, ter pri vseh ostalih aktivnostih, kjer se storitve oz. aktivnosti ne zagotavljajo po sistemu »time & material«.

Če posamezna storitev obsega več aktivnosti ali sodelovanje več izvajalcev, mora biti razvidna razčlenitev po posameznih aktivnostih in izvajalcih.

V primeru skupne ponudbe oziroma konzorcija, mora ponudnik priložiti tudi zbirno poročilo izvedenih aktivnosti po posameznih partnerjih konzorcija, iz katere mora biti razvidno kolikšen delež aktivnosti je v preteklem obdobju poročanja izvedel kateri izmed konzorcijskih partnerjev.

Zbirno poročilo o delovanju Interoperabilne hrbtenice in omrežja zNET:

- poročilo o doseženi zanesljivosti posameznih ključnih funkcionalnosti Interoperabilne hrbtenice,
- poročilo o doseženi zanesljivosti posameznih ključnih funkcionalnosti omrežja zNET,
- poročilo o obremenitvi posameznih delov sistema (zasedenost diskovnih podsistemov, procesorja, delovnega spomina,...),
- poročilo o odzivnosti posameznih delov sistema (povprečni/minimalni in maksimalni odzivni čas posameznih delov sistema,...),
- poročilo o veljavnosti digitalnih potrdil v uporabi rešitev eZdravja, in
- aktualni seznam uporabnikov oddaljenega dostopa.

Zbirno poročilo o izvedenih aktivnostih na področju SOC vsebuje:

- št. rešenih dogodkov na 1. ravni,
- št. rešenih dodatnih dogodkov / incidentov,
- varnostni incidenti segmentirani po kategorijah,
- varnostni incidenti segmentirani po stopnji kritičnosti,
- varnostni incidenti segmentirani po vrsti informacijskega vira,
- št. okuženih inf. virov,
- št. blokiranih virusov,
- št. virusnih okužb,
- št. zaznanih poskusov vdorov,
- št. blokiranih vdorov,
- št. incidentov s preseženim SLA, in
- št. kršenja varnostnih pravil (namerno/nenamerno).

Zraven navedenih poročil, mora ponudnik pripravljati tudi:

- zapisnike vseh sestankov, in
- redna poročila o zmogljivosti, zanesljivosti in varnosti sistema ter uporabljenih tehnologijah.

3.5.3 Koordinator izvedbe

Ponudnik mora za potrebe izvedbe storitvenih zahtevkov ter vodenja evidenc in poročanja zagotoviti strokovno usposobljenega Koordinatorja izvedbe, ki je odgovoren za koordinacijo vseh vpletenih deležnikov in nadzor nad pravočasno ter sledljivo izvedbo aktivnosti (zahtevkov) v skladu s procesi upravljanja in dogovorjenimi nivoji zagotavljanja storitev (SLA).

Naloge koordinatorja izvedbe zajemajo:

- koordinacija aktivnosti znotraj članov konzorcija,
- vodenje tehničnih in koordinacijskih sestankov ter priprava zapisnikov,
- izdelava rednih mesečnih poročil kot podlaga za mesečni obračun,
- priprava in usklajevanje posebnih poročil, letnih in pol letnih
- Priprava sodelovanje z zunanjimi izvajalci pri nadgradnji obstoječih rešitev,
- sodelovanje z zunanjimi izvajalci pri vključevanju novih rešitev,
- sodelovanje in usklajevanje z naročnikom, ter
- vodenje evidence obsega del iz naslova sodelovanja z zunanjimi izvajalci zaradi vključevanja novih rešitev ali nadgradenj obstoječih rešitev.

OPOMBA: Vlogo koordinatorja izvedbe lahko izvaja ista oseba, kot izvaja vlogo SLA managerja (glej poglavje 3.4), lahko pa gre za dva različna kadra.

3.5.4 Spremljanje obsega izvedenih del v okviru osnovnega vzdrževanja

Ponudnik mora ceno pavšala za Osnovno vzdrževanje določiti na način, da se sestoji iz fiksnega dela in variabilnega dela pavšala.

V fiksni del pavšala so vključene storitve, ki jih ponudnik izvaja po sistemu 24/7/365 in zajema:

- proaktivni nadzor delovanja omrežja NOC,
- zagotavljanje strokovnega osebja (kadrov) in pripravljenost izvajalca za potrebe zagotavljanja SLA,
- zagotavljanje kontaktnega centra, in
- zagotavljanje storitev operativnega centra kibernetskega varovanja SOC.

Navedene storitve fiksnega dela pavšala so v obrazcu »P-4: Predračun« zajete v postavkah »NOC storitve (FIKSNI DEL PAVŠALA)« (proaktivni nadzor delovanja omrežja), »SOC storitve (FIKSNI DEL PAVŠALA)« (operativni center kibernetskega varovanja) ter »Vodenje in usklajevanje reševanja incidentov in zahtevkov, vključno z zagotavljanjem kontaktnega centra ter strokovnega osebja in pripravljenosti za zagotavljanje SLA (FIKSNI DEL PAVŠALA)« (zagotavljanje kontaktnega centra ter zagotavljanje strokovnega osebja in pripravljenosti izvajalca za potrebe zagotavljanja SLA).

Preostanek pavšala za Osnovno vzdrževanje predstavlja mesečno naročnino za ocenjeno število opravljenih ur (na podlagi analize obsega aktivnosti v obdobju preteklih 12 mesecev znaša ocenjeno število ur na mesečnem nivoju **750 ur**) in predstavlja variabilni del mesečnega pavšala. Ponudnik mora v obrazec »P-4: Predračun« vnesti mesečno naročnino za izvajanje variabilnega dela pavšala v obsegu 750 ur, vrednost urne postavke pa se nato izračuna samodejno.

Variabilni del pavšala je v obrazcu »P-4: Predračun« zajet v postavki »Osnovno vzdrževanje – storitve (VARIABILNI DEL PAVŠALA)«, pri čemer je mesečna vrednost te postavke enaka zmnožku ocenjenega števila ur na mesec in ceni urne postavke v mesečni naročnini.

Naročnine in podpora proizvajalcev strojne in programske opreme iz obrazca »P-4: Predračun« niso del variabilnega dela pavšala in niso predmet kvartalnega poročila.

Ker je variabilni del mesečnega pavšala vzdrževanja določen na podlagi Tehničnih specifikacij (obrazec P-5), pri tem pa se lahko obseg storitev tekom izvajanja spremeni, bosta naročnik in

izvajalec kvartalno usklajevala dejansko število izvedenih ur dela s predvideno količino izvedenih ur dela v variabilnem delu mesečnega pavšala za osnovno vzdrževanje in v primeru odstopanj za več kot $\pm 10\%$ (deset odstotkov) izvajala poračun glede na dejansko opravljene storitve, kot sledi:

- V kolikor je dejansko število izvedenih ur višje od predvidenega za več kot 10% , je izvajalec opravičen do izdaje izredne fakture, pri tem pa se višina izredne fakture določi na način, da se preseženo število izvedenih ur (upoštevajo se ure nad 10% povečanjem obsega del) pomnoži z urno postavko v mesečni naročnini, ki je opredeljena v Prilogi P-4 predračun (glej: Urna postavka v mesečni naročnini);
- V kolikor je dejansko število opravljenih ur nižje od predvidenega za več kot 10% (deset odstotkov), je izvajalec obvezan naročniku izdati dobropis, pri tem pa se višina dobropisa določi na način, da se zmanjšano število izvedenih ur (upoštevajo se ure pod 10% zmanjšanjem obsega del) pomnoži z urno postavko v mesečni naročnini, ki je opredeljena v Prilogi P-4 Predračun (glej: Urna postavka v mesečni naročnini);

Za vodenje evidence vseh opravljenih ur dela je odgovoren Izvajalec, ki mora o tem mesečno poročati naročniku, skladno s točko 3.5.2 Vodenje evidenc in poročanje in določili pogodbe. Naročnik in izvajalec na podlagi poročil izvajalca ob koncu posameznega kvartala sporazumno uskladita in potrdita skupno število izvedenih ur, kar je osnova za izvedbo kvartalnega poračuna.

Za namen kvartalnega poračuna se dejansko število izvedenih ur v posameznem koledarskem četrtletju primerja s predvidenim številom ur, ki znaša trikratnik ocenjenega mesečnega števila ur iz obrazca »P-4: Predračun«. Odstopanje se ugotavlja na ravni celotnega četrtletja in ne po posameznih mesecih.

Pri poračunu se upoštevajo izključno ure, ki so evidentirane v sistemu za upravljanje zahtevkov, imajo enolično oznako aktivnosti in dokazilo o izvedbi skladno s poglavjem 3.5.2 teh Tehničnih specifikacij. Ure, ki niso evidentirane na navedeni način, se ne priznajo. Izjema iz poglavja 3.5.2, ki se nanaša na izvajanje storitev s strani timov, velja le glede navedbe posameznega kadra, ne pa tudi glede obsega opravljenih ur, ki mora biti izkazan tudi pri tiskem delu.

Če pogodbeni stranki skupnega števila ur ne uskladita v 30 (tridesetih) dneh po izteku četrtletja, se za namen poračuna upošteva število ur, izkazano v mesečnih poročilih izvajalca, ki jih je naročnik potrdil.

Naročnik ima ves čas trajanja pogodbe in še dve leti po njenem prenehanju pravico do pregleda (revizije) evidenc opravljenih ur, vključno z vpogledom v izvirne zapise v sistemu za upravljanje zahtevkov. Izvajalec mora vpogled omogočiti v roku 8 (osmih) delovnih dni od pisne zahteve naročnika, evidence pa hraniti najmanj dve leti po prenehanju pogodbe.

Če dejansko število izvedenih ur v dveh zaporednih četrtletjih odstopa od predvidenega v isto smer za več kot 10% , pogodbeni stranki ocenjeno mesečno število ur za nadaljnje obdobje izvajanja pogodbe ustrezno prilagodita s pisnim dodatkom k pogodbi.

Skupna vrednost izrednih faktur iz naslova poračuna variabilnega dela pavšala v posameznem pogodbenem letu ne sme preseči 20% (dvajset odstotkov) vrednosti variabilnega dela pavšala za to pogodbeno leto. Poračuni v nobenem primeru ne smejo povzročiti preseganja skupne pogodbene vrednosti; morebitno preseganje je dopustno le na podlagi pisnega dodatka k pogodbi, sklenjenega skladno z 95. členom ZJN-3.

3.6 Nadzor nad delovanjem informacijske rešitve

Izvajalec je dolžan upravljati in vzdrževati naročnikovo strojno in programsko opremo, s katero bo izvajal upravljanje in nadzor nad vsemi deli interoperabilne hrbtenice in omrežja zNET (strežniška infrastruktura, izmenjevalno vozlišče, CBP, komunikacijska oprema,...).

Izvajalec mora skrbeti za pravilno delovanje naročnikove programske opreme, s pomočjo katere bo lahko verodostojno spremljal, beležil in poročal o doseganju zanesljivosti in odzivnosti storitve, o zasedenosti kapacitet (strežnikov, diskovnega podsistema, delovnega spomina, ...).

Programska oprema za spremljanje delovanja storitve je zagotovljena s strani naročnika (Check MK) in zagotavlja:

- spremljanje (in obveščanje) obremenjenosti posameznega sistema ali systemskega sklopa (diskovne kapacitete, obremenitve strežnikov, obremenitve delovnega spomina, ...),
- možnost preverjanja delovanja posameznih strežniških servisov,
- možnost nadzora na aplikacijskem nivoju, in
- spremljanje varnosti na sistemskem nivoju
 - o nadzorni sistem za varnost na sistemskem nivoju skrbi za upravljanje z varnostnimi zapisi iz različnih virov informacijskega sistema (strežnikov, podatkovnih baz, požarnih pregrad,...),
 - o zapise mora hraniti ustrezno dolgo (vsaj 6 mesecev),
 - o izvajalec mora izvajati korelacijo varnostnih dogodkov, učinkovito zaznavati grožnje in napade v realnem času ter poročati o stanju systemske varnosti (skladnost s politikami).

Zahtevane frekvence izvajanja nadzora delovanja sistema:

Ključne storitve:	vsaj 1 krat na 60 sekund
Pomembne storitve:	vsaj 1 krat na 180 sekund
Ostale storitve:	vsaj 1 krat na 600 sekund (nadzor delovanja se bo izvajal na različnih nivojih odvisno od narave sistema, ki se ga nadzira)

Izvajalec mora vzpostaviti in za čas veljavnosti pogodbe za naprave v vzdrževanju zagotavljati nadzor naprav in povezav naročnika. Nadzorni sistem mora vključevati sledeče funkcionalnosti:

- spremljanje zasedenosti procesnih enot in ostalih pokazateljev obremenjenosti komunikacijskih naprav,
- spremljanje razpoložljivosti komunikacijskih naprav,
- spremljanje delovanja redundantnih napajalnikov, procesnih enot in sistemov hlajenja na centralnih stikalih,
- spremljanje zakasnitev in izgub paketov na povezavah,
- spremljanje razpoložljivosti povezav z upoštevanjem servisnih oken,
- spremljanje prometa na povezavah,
- spremljanje največje prepustnosti povezave v obeh smereh,
- spremljanje temperatur naprav ter alarmiranje v primeru preseganj kritičnih vrednosti,
- dnevno shranjevanje konfiguracij omrežnih naprav in arhiviranje do 10 njihovih različic,
- inventar spremljanih naprav s pregledom vseh gradnikov po posameznih lokacijah naročnika,

- spremljanje zastarelosti opreme in obveščanje naročnika o potrebnih zamenjavah,
- izdelava osnovnih in naprednih mesečnih poročil, in
- redno arhiviranje vseh izmerjenih podatkov.

Izvajalec mora v okviru storitve nadzora zagotavljati usposobljenega nadzornika, ki spremlja delovanje vseh naprav in servisov ter povezav v zNET omrežju. V primeru nenavadnih dogodkov, zaznanih težav in napak mora nadzornik v odzivnem času preko e-pošte, SMS ali telefona obvestiti kontaktne osebe naročnika. Sistem aktivnega nadzora z nadzornikom mora izvajalec zagotavljati od vse dni v letu v režimu 24/7.

Izvajalec bo s predmetnim naročilom za celotno obdobje veljavnosti pogodbe pri naročniku upravljal sistem za nadzor in upravljanje dogodkov CheckMK. Sistem kolektorja dogodkov je nameščen v okolju naročnika v redundantni postavitvi.

Upravljanje programske opreme CheckMK zajema:

- zmogljivost sistema nadziranja 60.000 servisov oziroma IKT virov,
- nadzor IKT virov in ključnih parametrov (SNMP, agent, ICMP, HTTP, Open Shift...),
- alarmiranje ob preseganju dogovorjenih vrednosti ali nedovoljenih stanj,
- obveščanje ob alarmu (e-pošte, SMS ali telefona obvestiti kontaktne osebe naročnika),
- poročila o razpoložljivosti naprav/storitev,
- integracija z evidenco za avtomatsko sinhronizacijo določenih naprav, in
- administracija sistema, spremljanje delovanja nadzornega sistema in izvajanje potrebnih prilagoditev skladno s spremembami IT okolja.

3.7 Licence za potrebe vzdrževanja infrastrukture eZdravja in omrežja zNET

Izvajalec mora v času trajanja pogodbe zagotoviti ustrezne licence za zagotavljanje podpore, kot sledi:

- naročnina za opremo CheckMK,
- naročnina za opremo IBM Qradar (SIEM),
- naročnina za opremo Citrix Netscaler,
- naročnina za opremo Data Protector,
- podpora za opremo HPE,
- podpora za opremo DELL,
- podpora za opremo IBM,
- podpora za opremo RedHat - Open Shift,
- podpora za opremo RedHat - Enterprise Linux,
- podpora za opremo Microsoft (Exchange, SQL),
- naročnina za opremo VEEAM MP for SCOM,
- naročnina za opremo VMware,
- naročnina za opremo Tenable,
- naročnina za opremo Fortra (Clearswift),
- naročnina za opremo Oracle Linux Premier Plus,
- naročnina za opremo Trend Micro,

- naročnina za opremo OpsLogix.

Ponudnik mora vse zahtevane licence zagotavljati v obliki mesečne naročnine, podrobnosti o zahtevanih nivojih podpore posameznega proizvajalca pa se nahajajo v zaupnem/zaprtem delu Tehničnih specifikacij, ki jih bo naročnik zainteresiranim ponudnikom poslal na zahtevo ob predložitvi podpisane izjave "P-10: Izjava o varovanju zaupne dokumentacije / Potrdilo naročnika".

OPOMBA: Podpore za programsko opremo proizvajalca Oracle ima naročnik zagotovljeno s pogodbo vzdrževanje preko Oracle Support-a in ni predmet tega javnega naročila.

3.7.1 Digitalna potrdila (certifikati)

Izvajalec mora v času trajanja pogodbe skladno s potrebami naročniku zagotavljati podporo pri pridobivanju in nameščanju SSL digitalnih potrdil (certifikatov), potrebnih za delovanje infrastrukture eZdravja, in sicer:

- predvidene količine in tipi potrebnih digitalnih potrdil se nahajajo v Prilogi št. 3: Potrošni material in digitalna potrdila*,
- v primeru izkazane potrebe mora ponudnik dotični certifikat iz Priloge 3 namestiti na namensko infrastrukturo eZdravja, skladno z zahtevami naročnika,
- po končani izvedbi bo naročnik ponudniku priznal 1 uro strokovnega dela iz naslova Dopolnilnega vzdrževanja, ki ga ponudnik obračuna na naslednjem mesečnem računu za izvedene storitve vzdrževanja.

* OPOMBA: v kolikor bi se tekom izvajanja pogodbe izkazalo, da potrebuje naročnik drugačna digitalna potrdila (certifikate) od navedenih v Prilogi 3, mora izvajalec naročniku nuditi podporo pri pridobivanju ponudb za nakup SSL digitalnih certifikatov s strani uveljavljenih ponudnikov (npr. Thawte, Geotrust, Digicert ...).

3.8 Varnostne in tehnološke zahteve ter zagotavljanje odzivnih časov (SLA)

Izvajalec mora vse storitve in aktivnosti izvajati na način, da bo zagotovljeno:

- ustrezna razpoložljivost sistema (tehnološke zahteve),
- ustrezna varnost (varnostne zahteve) in
- ustrezen odzivni čas v primeru nastalih težav (zahteve glede odzivnega časa in zagotavljane SLA),

skladno z zahtevami v nadaljevanju.

3.8.1 Varnostne zahteve

Zaščita pred zlonamerno kodo in zagotavljanje fizične, organizacijske in informacijske varnosti

Izvajalec mora zagotoviti zaščito vseh posameznih aplikacij, ki so vključene v projekt eZdravje pred zlonamerno kodo. Izvajalec je pri izvajanju opravil in aktivnosti storitev dolžan nenehno uveljavljati najboljše prakse s področij fizične, organizacijske in informacijske varnosti. Izvajalec je dolžan skrbno varovati podatke, s katerimi pride v stik pri izvajanju storitev.

Izvajalec mora svoje obveznosti izvajati v skladu s standardom ISO27001. Naročnik lahko napovedano ali nenapovedano izvede presojo fizične, organizacijske in informacijske varnosti po standardu ISO27001 in sicer v obsegu, ki je zahtevan za izvedbo pogodbe o izvajanju del, ki se dejansko izvajajo.

Varnostno kopiranje in povrnitev podatkov

Izvajalec mora zagotavljati avtomatizirano obnovitev delovanja brez izgube podatkov. Ciljni čas obnovitve delovanja je pet (5) minut.

Varnostno kopiranje mora:

- zagotavljati varnostno kopiranje različnih virov (datotečni sistem, podatkovne baze, virtualnih strežnikov),
- zagotavljati podporo za polni backup, neskončni inkrementalni backup, diferencialni backup, backup baze offline, online, backup log-ov,
- biti (popolnoma) avtomatizirano, tako da omogoča popolno ročno upravljanje, enostavno spreminjanje urnikov arhiviranja, enostavno upravljanje in ustrezno poročanje in obveščanje (elektronska pošta),
- uporabljati sodobne tehnologije za varnostno kopiranje (Disk To Disk, deduplikacija na strojni opremi),
- zagotavljati dolgotrajni iznos varnostnih kopij na trakove in virtualizacijo virov (ciljnih medijev), in
- omogočati stiskanje (kompresijo), šifriranje, ter Lan Free Backup.

Omejitev dostopov

Dostop do strežnike infrastrukture mora biti omejen le na potrebne oz. predvidene posege, tako programske kot dostope upravljalvskega oz. operativnega osebja.

Dostop do podatkov, shranjenih znotraj vseh aplikacij interoperabilne hrbtenice eZdravja in omrežja zNET, mora biti omogočen in omejen na osnovi pravic dostopa uporabnikov informacijskega sistema eZdravje.

Pravice dostopa so opredeljene za vsako posamezno aplikacijo ali na nivoju posameznih podprojektov eZdravja.

Revizijska sled in enotna sinhronizacija časa

Programska oprema sistema interoperabilne hrbtenice eZdravje omogoča sledenje vsem dostopom oz. prijavam - tudi neuspešno izvedenim - in zapisovanje revizijskih sledi na varen način.

Revizijske sledi morajo omogočati rekonstrukcijo in ugotavljanje upravičenosti dostopov do podatkov. Za ta namen je v okviru IT storitve uporabljena enotna sinhronizacija časa.

Varovanje zasebnosti osebnih podatkov

Pri varovanju zasebnosti bolnika in njegovih osebnih podatkov mora Interoperabilna hrbtenica kot celota slediti zakonskim zahtevam:

- šifriran in digitalno podpisan prenos podatkov izven informacijskega sistema (npr. čezmejna izmenjava,...), in
- varovanje osebnih podatkov pred nepooblaščenim dostopom.

3.8.2 Tehnološke zahteve

Zahteve glede razpoložljivosti

Rešitev mora delovati v režimu 24/7 in biti uporabnikom razpoložljiva vsaj 99,8% (kar predstavlja 17,52 ur nenapovedanega izpada na letni, 86,4 minut na mesečni in 20,2 minut na tedenski ravni).

Zahteve glede zmogljivosti (odzivnosti);

- Razpoložljivost rešitve vpliva na proces zdravljenja pacientov in delo izvajalcev zdravstvenih storitev, zato mora rešitev ob normalnem delovanju omrežnih in sistemskih storitev delovati v realnem času in zagotavljati, da je ob normalnem delovanju omrežnih in sistemskih storitev odzivni čas pod 1 sekundo;
- Odzivni čas posameznih rešitev ne sme ob normalnem delovanju omrežnih in sistemskih storitev presegati 2 sekund.

3.8.3 Odzivni časi in zagotavljanje SLA

Izvajalec mora vzdrževanje izvajati skladno z zahtevanimi roki in v odvisnosti od prioritete. Pri tem je potrebno upoštevati tudi režime odprave napak, ki jih omogočajo posamezni proizvajalci opreme, posebni režimi izvajanja storitev pa so v veljavi tudi za izvajanje storitev varnostno operativnega centra (SOC). Osnovno infrastrukturo za izvajanje pomoči uporabnikom zagotovi izvajalec. Ta infrastruktura vključuje sistem za upravljanje klicev, telefaksov, elektronske pošte, SMS sporočil in podobno za klicni center ter sistem za upravljanje problemov.

S ciljem enotne obravnave in razumevanja metrik za zagotavljanje SLA, se uporabljajo naslednje definicije:

- **Incident** je definiran kot nedelovanje informacijske rešitve oziroma delovanje, ki ni v skladu z zahtevami, določenimi v specifikaciji rešitve, oziroma tistimi, ki so z izvajalcem naknadno sporazumno dogovorjene oziroma z navodili za uporabo informacijske rešitve. Incidenti se delijo glede na resnost in vpliv na poslovanje, od česar je odvisna tudi hitrost oziroma nujnost odprave.
- **Odzivni čas** je čas, ki preteče od prejema prijave napake, do trenutka, ko izvajalec začne z odpravo napake, bodisi na lokaciji ali preko oddaljenega dostopa .

- **Povrnitev delovanja storitve** je čas od trenutka, ko so storitve za končne uporabnike spet operativne. Ob tem je incident lahko rešen z uporabo ekvivalentne opreme, spremembo konfiguracije ali drugo obhodno (workaround) metodo.
- **Čas odprave napake** je čas od prijave napake do njene končne odprave, bodisi zamenjava opreme, nadgradnja sistemske programske opreme, sprememba konfiguracije itd.
- **Čas izvajanja vzdrževanja** je čas ko izvajalec izvaja aktivnosti vzdrževanja na lokaciji, preko oddaljenega dostopa, v svojem laboratoriju in podobno.

Če izvajalec po pregledu prijave napake ugotovi, da bo za njeno odpravo potrebno več časa, kot je čas odprave napake, ki je podan v preglednici, je dolžan to nemudoma sporočiti naročniku in za vmesni čas vzpostaviti začasno delovanje informacijske rešitve, tako da bo delovni proces uporabnika omogočen.

Minimalni odzivni časi, ki jih mora v okviru vzdrževanja zagotavljati Izvajalec za odpravo napake po prijavi s strani naročnika, uporabnika ali prvega nivoja podpore so prikazani v spodnji tabeli. V kolikor Izvajalec v predpisanih minimalnih odzivnih časih ne vzpostavi funkcionalno stanje informacijskega sistema, se zaračuna pogodbeni kazni v višini, kot je opredeljeno v pogodbi. Za to vrednost se zmanjša znesek mesečnega pavšala za vzdrževanje.

Zahteve glede odzivnega časa pri reševanju zahtevkov

Izvajalec bo pri opravljanju storitev osnovnega vzdrževanja zagotovil reševanje zahtevkov v primeru napak oz. motenj pri delovanju, glede na njihovo prioriteto, ki se določi glede na vpliv napake oz. motnje na delovanje informacijske rešitve oz. delo uporabnikov. Odzivnimi časi za posamezni tip prioritete so navedeni v spodnji tabeli:

Prioriteta zahtevka	Odzivni čas	Čas, v katerem mora izvajalec odpraviti vzroke za napako oz. motnjo (če je v okviru zmožnosti izvajalca)*
kritična	1 ura	2 uri
visoka	2 uri	4 ure
pomembna	4 ure	8 ur
nizka	1 delovni dan	2 delovna dneva

Odzivni časi v primeru zahtevkov zaradi napak oz. motenj

** OPOMBA: Pri tem se v okviru merjenja doseganja zahtevanih nivojev SLA kot čas za rešitev težave upošteva »povrnitev delovanja storitve«, saj so v tem primeru storitve za končne uporabnike že operativne, končna odprava napak pa se izvede v najkrajšem možnem času in v skladu z režimi odprave napak, ki jih omogočajo posamezni proizvajalci opreme. Isti kazalnik, to je »povrnitev delovanja storitve«, je podlaga za obračun pogodbene kazni zaradi prekoračitve časovnih enot iz te preglednice.*

Opis stopnje prioritete:

Napaka / stopnja prioritete	Vpliv	Opis
kritična	zelo visok vpliv	Popolna odpoved delovanja storitev ali poglobitnega dela storitev, ki preprečuje uporabo ključnih delov informacijske rešitve vsem uporabnikom.
visoka	visok vpliv	Delna odpoved delovanja storitev ali poglobitnega dela storitev, ki resno vpliva na uporabo ključnih delov informacijske rešitve skupini uporabnikov.
pomembna	srednji vpliv	Oteženo delovanje storitev, ki ne vpliva kritično na uporabo ključnih delov informacijske rešitve pri skupini ali posameznem uporabniku.
nizka	nizek vpliv	Katerikoli incident, ki ne vpliva na uporabo ključnih delov informacijske rešitve.

Določitev stopnje prioritete napake

V primeru prijave zahtevka, ki ima zelo visok vpliv na poslovanje uporabnika, mora naročnik/uporabnik o tem obvezno obvestiti izvajalca tudi preko telefonskega klica, preko e-sporočila oz. spletnega obrazca pa lahko uporabnik pošlje dodatne podatke, ki so potrebni za učinkovitejše reševanje zahtevka s strani izvajalca.

Prioriteto zahtevka zaradi napake oz. motnje določi naročnik (oz. v njegovem imenu prvi nivo podpore ali od naročnika pooblaščen osebe). V primeru, da izvajalec prioriteto zahtevka spremeni na podlagi njemu dostopnih informacij, je podrobno pojasnilo razlogov za znižanje stopnje prioritete zahtevka sestavni del poročila o izvajanju storitev.

Izvajalec je dolžan na vprašanja ponudnikov pri integraciji novih rešitev ali nadgradnji obstoječih podati odgovor na vprašanje najkasneje v enem (1) delovnem dnevu.

Odzivni čas za dopolnilno vzdrževanje:

V primeru povpraševanj naročnika za dopolnilno vzdrževanje, je ponudnik dolžan pripraviti podrobno ponudbo (skupaj z oceno obsega del) najkasneje v treh (3) delovnih dnevih, v kolikor ni pisno dogovorjeno drugače.

3.8.3.1 Vzdrževanje opreme proizvajalca Cisco in CheckPoint

Kot je že navedeno, je potrebno zraven splošno definiranih rokov za odpravo napak, upoštevati tudi specifične (režime odprave napak), vezane na posameznega proizvajalca opreme. Navedeno velja v primeru, če ti roki odstopajo od splošno definiranih rokov.

Oprema Cisco:

Cisco oprema, podrobneje opredeljena v zaupnem / zaprtem delu dokumentacije (Priloga 2), je vključena v vzdrževanje po režimih glede na lokacijo in tip opreme:

- **Režim 1** – Cisco oprema, podatkovno računalniški center PRC 1 (Ljubljana)
- **Režim 2** – Cisco oprema, podatkovno računalniški center PRC 2 (Maribor)
- **Režim 3** – Cisco ISR usmerjevalniki (pri večjih izvajalcih)
- **Režim 4** – Cisco usmerjevalniki brez proizvajalčeve podpore (pri manjših izvajalcih)

Režim vzdrževanja Cisco opreme

Izvajalec mora izvajati vzdrževanje navedene Cisco opreme skladno z režimi v tabeli »Režim delovanja Cisco opreme«:

REŽIM	ODZIVNI ČAS	POVRNITEV STORITVE (REŠITEV INCIDENTA)	ČAS ODPRAVE NAPAKE	ČAS IZVAJANJA VZDRŽEVANJA	TEHNIČNA PODPORA PROIZVAJALCA	REZERVNA OPREMA
1	1 ura	2 ure	naslednji delovni dan	24 ur x 365 dni	DA	izvajalec
2	1 ura	4 ure	naslednji delovni dan	24 ur x 365 dni	DA	izvajalec
3	1 ura	4 ure	naslednji delovni dan	24 ur x 365 dni	DA	naročnik
4	1 uri	4 ure	naslednji delovni dan	24 ur x 365 dni	NE	naročnik

Režim delovanja Cisco opreme

Storitev v **režimu 1 in 2** mora vključevati vse potrebne nadomestne dele, material, potne stroške in delo potrebno za odpravo okvare v omrežju.

Storitev v **režimu 3 in 4** mora vključevati potne stroške in delo potrebno za odpravo okvare v omrežju.

Rezervno opremo za režima 1 in 2 zagotavlja izvajalec iz svojega lastnega skladišča rezervne opreme ter preko tehnične podpore proizvajalca.

Rezervno opremo za režim 3 in 4 zagotavlja naročnik iz svoje zaloge.

Oprema CheckPoint:

Za CheckPoint varnostno infrastrukturo mora biti zagotovljena proizvajalčeva podpora v okviru naročnine Collaborative Enterprise Support. Podpora vključuje tehnično pomoč, dostop do posodobitev in nadgradenj ter možnost uporabe podpornega portala.

Režim vzdrževanja, ki je vključen v proizvajalčevo podporo:

- 24x7 za kritične incidente,
- 8x5 za nižje prioritete incidentov,
- rezervni deli na voljo pri izvajalcu naslednji delovni dan po potrditvi napačnega delovanja ali nedelovanja opreme s strani CheckPoint TAC centra.

3.8.3.2 Dogovor o ravni storitve varnostno operativnega centra - SOC

Kot je že navedeno, je potrebno zraven splošno definiranih rokov za odpravo napak, upoštevati tudi posebni režimi izvajanja storitev varnostno operativnega centra (SOC), kot sledi:

Triažiranje:

Kategorija varnostnega dogodka	Odzivni čas triažnega postopka	
	Osnovni odzivni čas – proces triažiranja (oddaljeno)	Merilo uspešnosti izvedbe (operativna metrika)*
Manjši VD - Low (MR 1 - 2)	60 minut	80%
Srednji VD - Medium (MR 3 - 5)	45 minut	85%
Večji VD - High (MR 6 - 8)	30 minut	90%
Kritični VD - Critical (MR 9 - 10)	15 minut	95%
*merilo uspešnosti izvedbe predstavlja delež predčasno obravnavanih varnostnih dogodkov v triažnem postopku.		

Odzivni časi triaže

Kategorija varnostnega dogodka	Odzivni čas prve ravni	
	Prva raven - Upravljanje varnostnih dogodkov (oddaljeno)	Merilo uspešnosti izvedbe (operativna metrika)*
Manjši VD - Low (MR 1 - 2)	24 ur	80%
Srednji VD - Medium (MR 3 - 5)	8 ur	85%
Večji VD - High (MR 6 - 8)	2 uri	90%
Kritični VD - Critical (MR 9 - 10)	Neposredno nadaljevanje	95%
*merilo uspešnosti izvedbe predstavlja delež predčasno obravnavanih varnostnih dogodkov na prvi ravni podpore.		

Odzivni čas in merilo uspešnosti prve ravni

3.9 Postopki ob prevzemu in predaji del

Postopki ob prevzemu del oziroma uvedbi/pričetku izvajanja storitev

Izvajalec je dolžan po podpisu pogodbe in pred pričetkom izvajanja storitev v roku, za katerega se dogovori z naročnikom, ki ni daljši od 30 dni od podpisa pogodbe, izvesti naslednje:

- pripraviti opise postopkov po posameznih poglavjih/kategorijah storitev,
- izdelati navodila za svoje kadre za izvajanje del,
- pripraviti kontaktne naslove,
- izvesti interno uvajanje svojih kadrov za izvajanje del na naročnikovih upravljavskih in nadzornih sistemih,
- izvesti preizkus delovanja integracije z naročnikovimi evidencami in informacijskimi sistemi.

Naročnik izvede presojo pripravljanih del in v primeru, da so skladna s pogoji naročila in pogodbenimi določili naroči/odobri izvajalcu pričetek izvajanja storitev. V nasprotnem zahteva od izvajalca izvedbo korektivnih ukrepov.

Ob pričetku izvajanja storitev naročnik izvajalcu preda vse potrebne podatke in dostopna pooblastila potrebna za izvajanje del.

Vsi stroški, ki nastanejo v zvezi s pripravo in prevzemom izvajanja del, bremenijo izvajalca.

Vzpostavitev storitve varnostno operativnega centra - SOC

Trenutno naročnik že ima vzpostavljeno storitev SOC, ki jo bo moral zagotavljati tudi nov ponudnik po tem javnem naročilu. V sled navedenega morajo ponudniki predvideti tudi storitve vzpostavitev izvajanja operacije SOC, ki zajema vsaj priprava načrta uvedbe SOC operacije in vzpostavitev SOC operacije.

Načrt uvedbe SOC operacije

Naročnik pričakuje, da bo ponudnik s svojo metodologijo vsebinsko izpolnil vsaj naslednje zahteve:

- analiza IKT sistema,
- pregled analize poslovnih učinkov (BIA),
- pregled analize tveganj,
- pregled analize sistema SUVI (Sistem upravljanja in varovanja informacij),
- pregled načrta neprekinjenega poslovanja,
- pregled skladnosti varnostnih politik glede na zakonodajo ter regulative,
- definiranje obsega in načina varovanja gradnikov IKT sistema naročnika z opredelitvijo potrebnih nastavitve virov:
 - o vzpostavitev pravno formalnega okvirja za delovanje SOC operacije
 - o pregled in prilagoditev varnostnih politik, pravilnikov
 - o priprava predloga protokola obveščanja
 - o priprava standardnih operativnih postopkov (za izvajalca SOC, naročnika in naročnikove pogodbene partnerje)
- izdelava RACI matrike

Vzpostavitev SOC operacije

Uspešen zagon operativne storitve SOC vključuje najmanj naslednje aktivnosti:

- vzpostavitev varnega oddaljenega dostopa SOC ponudnika do IT sistema naročnika,
- prevzem upravljanega sistema SIEM,
- integracija orodij naročnika, ki so potrebni za izvajanje SOC operacije,
- navezava gradnikov informacijskega sistema naročnika na SOC sistem,
- vzdrževanje in nadgradnja obstoječih pravil (npr. SIEM korelacije),
- osnovne nastavitve obveščanja in poročanja, in
- redno izvajanje operativnih storitev SOC.

Pripravljen, potrjen in predan projektna dokumentacija ter pogoj za pričetek izvajanja SOC

Pred pričetkom izvajanja storitev vzdrževanja po tem javnem naročilu, mora Izvajalec:

- naročniku predati vso zahtevano tehnično dokumentacijo in navodila (skladno z zahtevami tega javnega naročila), ter
- uspešno zaključiti poskusno obratovanje celovite storitve Operativne kibernetске zaštite (SOC) z odpravljenimi vsemi ugotovljenimi pomanjkljivostmi, poročili in rednimi koordinacijami izvajalca storitev in naročnika.

3.10 Zagotavljanje potrošnega materiala in digitalnih potrdil

Izvajalec mora v svojo ponudbo vključiti potrošni material in zahtevana digitalna potrdila, kar vse se bo potrebovalo tekom izvajanja pogodbe, pri tem pa končne količine in dinamika porabe še niso časovno opredeljene.

V sled navedenega mora ponudnik v svoji ponudbi opredeliti cene na enoto posameznega kosa potrošnega materiala in digitalnih potrdil, ki morajo biti veljavne celotno trajanje pogodbe.

Specifikacija potrošnega materiala in digitalnih potrdil ter predvidene količine se nahajajo v »Prilogi št. 3: Potrošni material in digitalna potrdila«, pri tem pa se naročnik ne obvezuje, da bo tekom izvajanja pogodbe tudi dejansko naročil vse predvidene količine.

Naročnik lahko v primeru izkazanih potreb naroča tudi potrošni material in digitalna potrdila, ki niso na seznamu. V tem primeru izvajalec pripravi posebno ponudbo, ponujene cene pa ne smejo bistveno odstopati od cen na trgu.

Ponudnik mora v svoji ponudbi priložiti tehnične specifikacije ponujenega materiala. Ker se lahko tekom izvajanja pogodbe proizvajalci in modeli ponujenega potrošnega materiala menjajo, bo naročnik kot primeren potrošni material priznal tudi primerljive modele potrošnega materiala, kot jih bo ponudnik predvidel ob oddaji ponudbe, pri tem pa se cena na enoto potrošnega materiala ne sme spremeniti.

Priloga 1: Storitve vzdrževanja in upravljanja omrežja zNET

Upravljanje fizičnega in logičnega nivoja omrežja

Upravljanje fizičnega in logičnega sloja omrežja predstavlja upravljanje strojne in programske opreme gradnikov omrežja zNET. Upravljanje fizičnega sloja - gradnikov omrežja obsega:

- bakrenih povezav,
- optičnih povezav,
- vmesnikov za optična vlakna, pretvornikov in koncentradorjev,
- Ethernet stikal,
- usmerjevalnikov,
- centralnih požarnih pregrad, in
- nadzorni in upravljavski sistemi (ang.: »Management systems«, ang.: »Network Monitoring Systems«).

Upravljanje logičnega sloja predstavlja upravljanje L2, L3 in L4 slojev ISO/OSI protokolnega sklada, zagotavljanje usmerjanja TCP/IP prometa v omrežju zNET, zagotavljanje varnosti in visoke razpoložljivosti v omrežju zNET.

Upravljanje programske opreme aktivnih elementov omrežja predstavlja zagotavljanje optimalne programske in strojne opreme aktivnih gradnikov omrežja.

Upravljanje in vzdrževanje vse opreme na končnih lokacijah, ne glede na lastništvo, izbran način priklopa ali ponudnika telekomunikacijskih storitev.

Procesi upravljanja fizičnega in logičnega sloja omrežja zNET

V nadaljevanju se nahaja specifikacija aktivnosti, ki jih je potrebno izvajati v okviru posameznih procesov.

Priklop nove lokacije po naročilu:

- prevzem opreme iz operativnega skladišča ali pri dobavitelju,
- konfiguracija opreme na osnovi vnaprej določenih parametrov,
- konfiguracija opreme na osnovi vnaprej določenih parametrov - zahtevna lokacija (več ZD ali lokalnih omrežij hkrati),
- instalacija in priklop opreme (vgradnja v komunikacijsko omaro, priključitev ustrezno napajanje, priklop na naročeno povezavo »upstream« in priklop na LAN »access«),
- preizkus delovanja – povezljivosti v obe smeri,
- vpis vozlišča in opreme v evidenco naprav in v nadzorni in upravljavski sistem,
- priprava kvartalnih poročil o novih lokacijah.

Ukinitev obstoječe lokacije:

- de-instalacija opreme (izklop opreme iz ustreznega napajanja, odklop povezave, odklop LAN povezave, deinstalacija opreme iz komunikacijske omare),
- ustrezna evidenca opreme,
- priprava kvartalnih poročil o ukinjenih lokacijah.

Prestavitev obstoječe lokacije na novo lokacijo (po naročilu):

- de-instalacija opreme na stari lokaciji (izklop opreme iz ustreznega napajanja, odklop povezave, odklop LAN povezave, deinstalacija opreme iz komunikacijske omare),
- ustrezna prekonfiguracija opreme na osnovi vnaprej določenih parametrov,
- instalacija in priklop opreme na novi lokaciji (vgradnja v komunikacijsko omaro, priključitev ustreznega napajanja, priklop na naročeno povezavo »upstream« in priklop na LAN »access«),
- preizkus delovanja – povezljivosti v obe smeri. Ustrezna evidenca vozlišča in opreme v evidenco naprav v nadzornem in upravljalnem sistemu Kvartalna poročila o prestavljenih lokacijah.

Zagotavljanje delovanja naprav in povezav:

- prevzem incidenta,
- ugotavljanje napake – začasna rešitev incidenta Odprava napake – končna rešitev incidenta priprava poročil o incidentih,
- preverjanje dosegljivosti delov omrežja in delovanje naprav na tej poti.

Spremljanje delovanja povezav:

- preverjanje prepustnosti povezav (Network Monitoring system),
- poročilo o preobremenjeni povezavi in njenih vzrokih,
- priprava poročila (statistika) o delovanju povezav.

Spremljanje delovanja in upravljanje IP/Ethernet gradnikov omrežja

- konfiguracija parametrov IP/Ethernet gradnikov omrežja,
- arhiviranje konfiguracij aktivne opreme,
- pregled in analiza log datotek aktivne opreme (preventivni pregledi),
- priprava poročila o nedelujoči in/ali slabo delujoči opremi,
- priprava predloga izboljšave delovanja aktivne opreme,
- nadgradnja programske opreme na zahtevo naročnika,
- priprava poročila o delovanju IP/Ethernet gradnikov omrežja.

Koordinacija priklopa s ponudniki storitev:

- koordinacija priklopa lokacije s ponudnikom storitev,

- poročila koordinacij s ponudnikom storitev (kvartarno).

Administracija dostopa uporabnikov z oddaljenim dostopom do lokalnih omrežij:

- administracija dostopa uporabnika oddaljenega dostopa do LAN omrežja in do zahtevanih strežnikov,
- vpis uporabnika v evidenco opreme in naprav.

Upravljanje operativnega skladišča:

- vodenje operativnega skladišča,
- nadgradnje firmware-a in programske opreme na uskladiščeni aktivni opremi po naročilu naročnika,
- priprava poročila o operativnem skladišču (kvartalno).

Dežurstvo – pripravljenost:

- pripravljenost na domu oziroma na lokaciji, iz katere je možno vzpostaviti VPN povezavo.

Vzdrževanje osrednjih komunikacijskih vozlišč in sistemskih prostorov:

- administracija – povezovanje in prevezovanje naprav v sistemskih prostorih naprav,
- administracija – povezovanje in prevezovanje naprav v komunikacijskih vozliščih,
- nepredvidljive naloge (po naročilu),
- analiza po potrebi,
- priprava predloga rešitve,
- preizkus rešitve v laboratoriju,
- preizkus rešitve v testnem omrežju,
- implementacija rešitve v produkcijskem omrežju.

Upravljanje in zagotavljanje delovanja varnega sistema oddaljenega dostopa do omrežja

Upravljanje in zagotavljanje delovanja varnega sistema oddaljenega dostopa do omrežja zNET predstavlja upravljanje gradnikov sistema dostopa do omrežja zNET. Gradniki so podvojeni in postavljeni v visoki razpoložljivosti delovanja. Gradnike predstavlja strojna in programska oprema potrebna za oddajen dostop do omrežja zNET.

Strojna oprema:

- strojna oprema so strežniki na katerih je nameščena programska oprema za storitve RADIUS in LDAP in
- namenska (ang.: »appliance«) strojna oprema VPN koncentratorjev.

Programska oprema:

- programska oprema sistema enkratnih gesel in podatkovna baza,
- RADIUS programska oprema in podatkovna baza,
- LDAP programska oprema in podatkovne baze,
- programska oprema VPN koncentradorjev.

Procesi upravljanja in zagotavljanja delovanja varnega oddaljenega dostopa do omrežja zNET**Postavitev strežnika:**

- fizična instalacija strežnika v komunikacijsko omaro ter priklop na napajaje,
- priključitev strežnika na aktivno opremo,
- instalacija OS,
- optimizacija OS,
- test delovanja OS in povezljivost z omrežjem,
- instalacija potrebne programske opreme s potrebnimi nastavitvami – konfiguracijo,
- vpis stanja v evidenco naprav.

Upravljanje OS strežnika:

- arhiviranje potrebnih datotek za delovanje OS,
- pregledovanje dnevnikov (z ustreznim orodjem),
- priprava predlogov za nadgradnjo strežnika ali OS,
- nadgradnja strežnika ali OS po naročilu naročnika.

Upravljanje programske opreme TACACS:

- arhiviranje programske opreme in podatkovnih baz,
- upravljanje profilov uporabnikov,
- arhiviranje programske opreme in podatkovnih baz,
- priprava predloga nadgradnje programske opreme,
- nadgradnja programske opreme po naročilu naročnika.

Upravljanje programske opreme LDAP:

- upravljanje LDAP baze uporabnikov,
- priprava poročila o delovanju LDAP sistema (kvartarno),
- priprava predloga nadgradnje LDAP programske opreme,
- nadgradnja LDAP programske opreme po naročilu naročnika.

Upravljanje "appliance" opreme VPN koncentradorjev:

- arhiviranje programske opreme in podatkovnih baz Konfiguracija VPN koncentradorja,
- upravljanje VPN koncentradorja (spremljanje statistike in dnevnikov),
- priprava poročila o delovanju VPN koncentradorjev (mesečna, letna),
- priprava predloga nadgradnje programske opreme VPN koncentradorji,
- nadgradnja VPN programske opreme po naročilu naročnika.

Dežurstvo – pripravljenost:

- pripravljenost na domu oziroma na lokaciji, iz katere je možno vzpostaviti VPN povezavo.

Nepredvidljive naloge:

- analiza po potrebi,
- priprava predloga rešitve,
- preizkus rešitve v laboratoriju,
- preizkus rešitve v testnem omrežju,
- implementacija rešitve v produkcijskem omrežju.

Upravljanje in zagotavljanje varnostnih sistemov v omrežju

Upravljanje in zagotavljanje varnostnih sistemov v omrežju zNET, predstavlja upravljanje gradnikov varnostnih sistemov v omrežju zNET. Gradnike predstavljajo požarne pregrade in oprema za odkrivanje in preprečevanje vdorov. Gradniki so podvojeni in postavljeni v visoki nivo razpoložljivosti. Gradnike predstavlja strojna in programska oprema potrebna za požarne pregrade in oddaljen dostop do omrežja zNET.

Strojna oprema:

- strojna oprema so strežniki na osnovi Linux/Unix OS na katerih je instalirana programska oprema za požarne pregrade,
- »Appliance« požarne pregrade,
- strežniki na katerih je instalirana programska oprema za upravljanje IDP sistemov za odkrivanje in preprečevanje vdorov,
- strežniki na katerih je instalirana podatkovna baza potrebna za IDP sistem za odkrivanje in preprečevanje vdorov.

Programska oprema:

- namenska programska oprema požarnih pregrad - programska oprema za požarne pregrade,
- namenska programska oprema požarnih pregrad – namenska (ang.: »appliances«) programska oprema,
- namenska programska upravljavska oprema požarnih pregrad - programska oprema za upravljanje požarnih pregrad,

- namenska programska oprema za preprečevanje vdorov - programska oprema za upravljanje sistemov za odkrivanje in preprečevanje vdorov.

Procesi upravljanja in zagotavljanja delovanja varnostnih sistemov v omrežju zNET:

Postavitev strežnika:

- fizična instalacija strežnika v komunikacijsko omaro ter priklop na napajanje,
- priključitev strežnika na aktivno opremo,
- instalacija OS,
- optimizacija OS,
- test delovanja OS in povezljivost z omrežjem,
- instalacija potrebne programske opreme s potrebnimi nastavitvami – konfiguracijo,
- vpis strežnika v evidenco naprav.

Upravljanje OS strežnika:

- arhiviranje potrebnih datotek za delovanje OSa
- pregledovanje dnevnikov (z ustreznim orodjem)a
- priprava predlogov za nadgradnjo OS,
- nadgradnja OS po naročilu naročnika.

Postavitev appliance – naprave:

- fizična instalacija namenske "appliance" naprave v komunikacijsko omaro,
- priključitev naprave na ustrezno napajanje,
- priključitev naprave na aktivno opremo,
- konfiguracija namenske "appliance" opreme,
- vpis naprave v evidenco naprav.

Upravljanje programske opreme za nadzor požarnih pregrad:

- arhiviranje podatkovne baze nadzora požarnih pregrad,
- pregledovanje dnevnikov delovanja nadzora požarnih pregrad,
- priprava predloga nadgradnje nadzora požarnih pregrad,
- nadgradnja programske opreme nadzora požarnih pregrad po naročilu naročnika.

Upravljanje požarnih pregrad:

- konfiguriranje delovanja požarne pregrade (usmerjanje,...),
- spreminjanje varnostnih pravil,
- dodajanje varnostnih pravil,
- odzemanje varnostnih pravil,

- preverjanje varnostnih pravil,
- priprava poročil o delovanju, razpoložljivosti in prometu na požarnih pregrad (mesečno in letno).

Upravljanje programske opreme za upravljanje IDP sistema:

- arhiviranje podatkovnih baz in programske opreme,
- pregled dnevnikov,
- analiza dnevnikov,
- namestitve novih alarmov in pravil,
- preizkus novih alarmov in pravil po namestitvi Forenzične analize na osnovi naročila naročnika,
- priprava predloga nadgradnje programske opreme,
- nadgradnja programske opreme na osnovi naročila naročnika,
- priprava poročil o delovanju IDP sistema (mesečno in letno).

Upravljanje programske opreme za upravljanje varnosti strežnikov / delovnih postaj:

- arhiviranje podatkovnih baz in programske opreme,
- pregled dnevnikov varnosti delovnih postaj,
- analiza dnevnikov varnosti delovnih postaj,
- namestitve novih alarmov in pravil,
- preizkus novih alarmov in pravil po namestitvi,
- priprava predloga nadgradnje programske opreme,
- nadgradnja programske opreme na osnovi naročila naročnika,
- priprava poročila o delovanju programske opreme varnosti delovnih postaj (mesečna in letna).

Dežurstvo – pripravljenost:

- pripravljenost na domu oziroma na lokaciji, iz katere je možno vzpostaviti VPN povezavo.

Nepredvidljive naloge:

- analiza po potrebi,
- priprava predloga rešitve,
- preizkus rešitve v laboratoriju,
- preizkus rešitve v testnem omrežju,
- implementacija rešitve v produkcijskem omrežju.

Upravljanje in zagotavljanje pomožnih servisov za delovanje omrežja

Upravljanje in zagotavljanje pomožnih servisov za delovanje omrežja zNET predstavlja upravljanje strojne in programske opreme za delovanje servisov, potrebnih za nemoteno delovanje storitev in omrežja zNET.

Strojna oprema:

- strojno opremo predstavljajo strežniki na osnovi Linux/Unix OS.

Programska oprema:

- programska oprema imeniških servisov (»DNS «),
- programska oprema posredovalnih servisov (»Proxy / Cache«),
- programska oprema za beleženje dogodkov (»syslog«),
- programska oprema nadzornih sistemov in sistemov za spremljanje delovanja omrežja (ang. »Network monitoring«),
- programska oprema za sporočilni sistem tehničnih pregledov,
- podatkovna baza objektov omrežja zNET,
- sistem za izvajanje korelacij log zapisov,
- podatkovna baza konfiguracij usmerjevalnikov in stikal omrežja zNET (upravljavski sistem).

Procesi upravljanja in zagotavljanja pomožnih servisov za delovanje omrežja zNET:**Postavitev strežnika:**

- fizična instalacija strežnika v komunikacijsko omaro ter priklop na napajanje,
- priključitev strežnika na aktivno opremo,
- instalacija OS Optimizacija OS,
- test delovanja OS in povezljivost z omrežjem,
- instalacija potrebne programske opreme s potrebnimi nastavitvami – konfiguracijo,
- vpis strežnika v evidenco naprav.

Upravljanje OS strežnika:

- arhiviranje potrebnih datotek za delovanje OS,
- pregledovanje dnevnikov (z ustreznim orodjem),
- priprava predlogov za nadgradnjo strežnika ali OS,
- nadgradnja strežnika ali OS po naročilu naročnika.

Upravljanje DNS programske opreme – upravljanje zunanjih in notranjih domen zdravstvenih zavodov:

- dodajanje novih domen,
- brisanje domen,
- dodajanje elementov v domenah,
- brisanje elementov v domenah,
- poprava vpisanih elementov,
- pregledovanje dnevnikov,
- priprava predloga za nadgradnjo,
- nadgradnja programske opreme po naročilu naročnika,

- priprava poročila o delovanju DNS storitve.

Upravljanje proxy/cache programske opreme:

- spremljanje zasedenosti proxy/cache strežnikov,
- spreminjanje konfiguracijske datoteke po naročilu naročnika,
- priprava predloga nadgradnje programske opreme,
- nadgradnja programske opreme po naročilu naročnika,
- priprava poročila o delovanju proxy/cache storitve (mesečna in letna).

Upravljanje Syslog programske opreme:

- spremljanje zasedenosti Syslog strežnikov,
- pregledovanje dnevnikov,
- priprava poročila o zasedenosti Syslog strežnikov (kvartalno).

Upravljanje Network monitoring sistema:

- arhiviranje konfiguracije Network Monitoring sistema,
- posodabljanje baze objektov za Network Monitoring sistem,
- administracija Network Monitoring Systema – prilagajanje glede na zahteve omrežja,
- spremljanje dnevnikov,
- poročanje o delovanju Network Monitoring sistema (kvartalno).

Upravljanje sporočilnih sistemov:

- arhiviranje baze in konfiguracije poštnega sistema,
- spremljanje dnevnikov,
- administracija uporabnikov poštnega sistema,
- pomoč uporabnikom poštnega sistema,
- poročanje o delovanju poštnega sistema (kvartalno).

Upravljanje spletnih strežnikov:

- arhiviranje konfiguracije spletnih strežnikov,
- spremljanje dnevnikov spletnih strežnikov,
- administracija servisov spletnih strežnikov.

Upravljanje CA strežnika (MS):

- arhiviranje baze in konfiguracij CA sistema,
- spremljanje dnevnikov CA sistema,
- spremljanje zasedenosti strežnika,

- administracija CA sistema,
- priprava predloga nadgradnje programske opreme,
- nadgradnja programske opreme po naročilu naročnika,
- priprava poročila o delovanju CA storitve (kvartalna in letna).

Upravljanje strežnikov pretočnih vsebin:

- arhiviranje baz in konfiguracij strežnikov pretočnih vsebin,
- spremljanje dnevnikov strežnikov pretočnih vsebin,
- administracija servisov strežnikov pretočnih vsebin.

Upravljanje s podatkovno baza objektov omrežja zNET (evidenca naprav, organov, lokacij, ...):

- arhiviranje podatkovne baze objektov omrežja zNET,
- spremljanje dnevnikov,
- poročanje o delovanju in razpoložljivosti podatkovne baze objektov omrežja zNET (kvartalno).

Upravljanje s podatkovno baza konfiguracij usmerjevalnikov in stikal omrežja zNET (upravljavski sistem):

- arhiviranje podatkovne baze konfiguracij,
- spremljanje dnevnikov,
- poročanje o zasedenosti strežnika (kvartalno).

Dežurstvo – pripravljenost:

- pripravljenost na domu oziroma na lokaciji, iz katere je možno vzpostaviti VPN povezavo.

Nepredvidljive naloge :

- analiza po potrebi,
- priprava predloga rešitve,
- preizkus rešitve v laboratoriju,
- preizkus rešitve v testnem omrežju,
- implementacija rešitve v produkcijskem omrežju.

Priloga 2: Zaprti / zaupni del tehničnih specifikacij

Ker zaupni/zaprti del dokumentacije, ki obsega informacije o razporeditvi strojne opreme med lokacijama PRC 1 (Ljubljana) in PRC 2 (Maribor), podrobne informacije o strežniški in mrežni opremi ter ostale podrobne tehnične informacije, predstavlja poslovno skrivnost, bo naročnik ta del dokumentacije zainteresiranim ponudnikom poslal na zahtevo ob predložitvi podpisane izjave "P-10: Izjava o varovanju zaupne dokumentacije / Potrdilo naročnika", skladno s postopkom, opredeljenim v Navodilu ponudnikom predmetnega javnega naročila.

Priloga 3: Potrošni material in digitalna potrdila

V nadaljevanju se nahaja okvirni seznam rezervne opreme in potrošnega materiala ter predvidene količine (seznam lahko naročnik po potrebi dopolnjuje s primerljivimi produkti, ki morajo biti najmanj enake kakovosti oziroma kakovostnejši od prvotno navedenih produktov in se dobavljajo po enaki ceni):

Produktna št.	Opis	Ocenjena količina
STACK-T1-3M=	Cisco StackWise visoko-hitrostni kabel dolžine 3 m	10
STACK-T1-1M=	Cisco StackWise kabel dolžine 1 m	10
CAB-STACK-1M	Cisco StackWise kabel dolžine 1 m	10
CAB-SPWR-30CM	Cisco StackPower kabel dolžine 30 cm	2
PWR-C1-715WAC	Cisco 715W AC napajalni modul	4
PWR-C1-1100WAC	Cisco 1100W AC napajalni modul	2
CAB-AC-EU	Napajalni kabel C13–C14	6
8510067	Napajalni kabel C14–C15 dolžine 2 m	4
8510068	Napajalni kabel C14–C15 dolžine 1 m	4
8510035	Napajalni kabel C13–C14 dolžine 1,8 m	4
8510034	Napajalni kabel C13–C14 dolžine 1,2 m	4
SFP-H10GB-CU3M	10 Gbps SFP+ DAC kabel dolžine 3 m	6
SFP-H10GB-CU5M	10 Gbps SFP+ DAC kabel dolžine 5 m	4
SFP-10G-AOC10M	10 Gbps SFP+ AOC kabel dolžine 10 m	4
SFP-10G-SR	10 Gbps SFP+ SR optični modul (multimode, LC)	8
SFP-10G-LR	10 Gbps SFP+ LR optični modul (singlemode, LC)	2
SFP-10G-ER	10 Gbps SFP+ ER optični modul (singlemode, LC)	1
FO MM LC-LC 10m	Multimodni optični kabel LC–LC dolžine 10 m	10
LC UPC LC UPC OM4 2m	Multimodni optični kabel OM4 LC–LC dolžine 2 m	10
LC UPC LC UPC OM4 5m	Multimodni optični kabel OM4 LC–LC dolžine 5 m	10
LC UPC LC UPC OM4 10m	Multimodni optični kabel OM4 LC–LC dolžine 10 m	10
GLC-SX-MMD=	1 Gbps SFP modul SX (multimode, LC)	4
GLC-TE=	1 Gbps SFP modul RJ45 (UTP)	4
SFP-25G-SR-S	25 Gbps SFP28 SR optični modul (multimode)	4
SFP-25G-LR-S	25 Gbps SFP28 LR optični modul (singlemode)	2
QSFP-40G-SR4	40 Gbps QSFP+ SR optični modul (multimode, MPO)	2
QSFP-100G-SR4-S	100 Gbps QSFP28 SR optični modul (multimode, MPO)	2
CPT-SFP-10/25G-CSR-S	SFP28 25/10GB LC,300M, 850nm, DD kompatibilni	12
SFP28	XTM85P-M3LY-TC - kompatibilni	20
SSL/TLS	Strežniška digitalna potrdila	10

IZJAVA PONUDNIKA:

Spodaj podpisani, zastopnik/pooblaščenec ponudnika, ki se prijavlja na predmetno javno naročilo, izjavljam, da smo seznanjeni s pogoji, merili in ostalo vsebino razpisne dokumentacije za navedeno javno naročilo ter jih v celoti sprejemamo.

Hkrati izjavljam, da vse ponujene storitve v celoti ustrezajo Tehničnim specifikacijam, ter da bo vsa komunikacija z naročnikom potekala v slovenskem jeziku.

Kraj in datum:

Podpis odgovorne osebe in žig:
