Strokovne zahteve

NASLOV JN: Osnovno in dopolnilno vzdrževanje laboratorijskega informacijskega sistema v UKC Ljubljana

Točka	Opis	Količina
1	**Osnovno vzdrževanje za laboratorijski informacijski sistem (LIS) za obdobje 48 mesecev**	1
2	**Dopolnilno vzdrževanje laboratorijskega informacijskega sistema (LIS) za obdobje 48 mesecev**	1

*Točka 1 mora ponudnik oceniti kot mesečni strošek
*Točka 2 mora ponudnik oceniti kot strošek na ure dodatnega dela

1. Varnostne in skladnostne smernice

Izpolnjene morajo biti varnostne in skladnostne smernice, ki se nanašajo na direktivo NIS2.

Smernice so:

- Vsi uporabniki morajo imeti edinstvena uporabniška imena.
- Aplikacija ločuje navadne in privilegirane uporabniške račune.
- Nobeno uporabniško ime in/ali geslo ne sme biti vpisano neposredno v aplikacijo (hard-coded).
- Aplikacija mora omogočati dodeljevanje dostopa na podlagi vlog (role-based access control).
- Aplikacija mora omogočati implementirano stroge politike gesel. Uporabniška gesla morajo imeti najmanj 10 znakov in morajo biti ustrezne kompleksnosti (vsebovati vsaj eno malo črko, eno veliko črko in vsaj eno številko). Gesla je potrebno menjati minimalno vsakih 12 mesecev; 24 zaporednih gesel je neponovljivih; Geslo se zaklene za petnajst minut po petih nepravilnih poizkusih vnosa. Priporočamo uporabo AD uporabniških računov (SSO). Privilegirana uporabniška gesla zahtevajo višji nivo kompleksnost.
- Za vse privilegirane aktivnosti mora sistem zahtevati vsaj dvo-faktorsko avtentikacijo (2FA)še bolje več-faktorsko avtentikacijo (MFA).
- Aplikacija mora imeti uvedene mehanizme za spremljanje in evidentiranje dostopa uporabnikov do sistema.
- Aplikacija mora zagotavljati revizijske sledi dostopa do osebnih podatkov.
- Aplikacija mora biti razvita skladno s standardi, dobrimi praksami in smernicami ter zagotavljati visoko raven zaupnosti, celovitosti in razpoložljivosti podatkov.
- Vsi podatki morajo biti šifrirani med prenosom. Posebne vrste osebnih podatkov morajo biti šifrirane tudi ob hranjenju.
- Izvajalec mora redno izvajati varnostne preglede in revizije svojega razvojnega sistema, vključno z vdornimi testiranji.
- Izvajalec mora zagotavljati vse popravke in posodobitve, da zagotavljajo, zaščito pred znanimi ranljivostmi.

- Sodelovati mora pri preiskavah incidentov ter omogočiti forenzično zaščito podatkov.
- Izvajalec je dolžan poročati naročniku o varnostnih incidentih, ki bi lahko vplivali na delovanje UKCL. Ravno tako mora kot ključni dobavitelj kritičnemu subjektu zagotavljati skladnost z Zakonom o informacijski varnosti, vključno s poročanjem pristojnemu organu.
- Implementirane mora imeti požarne zidove in sisteme za preprečevanje vdorov (v primeru, da ima izvajalec v vzdrževanju tudi infrastrukturo-strežnik).
- Zagotoviti mora skladnost z zahtevami Informacijske varnostne politike, ki je skladna z zahtevami ISO/IEC 27001.
- Zagotoviti mora ustrezno upravljanje sprememb ter sledenje varnostnim popravkom in posodobitvam programske opreme.
- Imeti mora uveden sistem za upravljanje incidentov (ITIL).
- Vsi sistemi morajo imeti implementirane varnostne rešitve za zaščito pred zlonamerno programsko opremo (v primeru, da ima izvajalec v vzdrževanju tudi infrastrukturo-strežnik).
- Implementiran mora biti nadzor in beleženje vseh varnostnih dogodkov in dostopov. Sistemi morajo omogočati pošiljanje zapisov v centralni sistem za upravljanje dnevniških zapisov in dogodkov (SIEM) v eni od standardnih normaliziranih oblik (v primeru, da ima izvajalec v vzdrževanju tudi infrastrukturo-strežnik).
- Redno izvaja analize tveganj in prilagaja varnostne ukrepe.
- Vsi oddaljeni dostopi morajo biti varni, šifrirani in časovno omejeni skladno z zahtevami naročnika.
- Implementirane morajo biti politike za varnostno uničenje podatkov in strojne opreme, anonimizacijo in psevdonimizacijo osebnih podatkov, kjer je to potrebno zaradi zahtev ZVOP.
- Zagotavljati mora skladnost z vsemi relevantnimi zakoni in predpisi o kibernetski varnosti.
- Redno izvajanje varnostne ocene in preverjanja izvajalca.
- Zagotavljajo ustrezno varnostno kopiranje podatkov in redno preverjanje obnovljivosti teh kopij (v primeru, da ima izvajalec v vzdrževanju tudi infrastrukturo-strežnik).
- Redno preverjajo in posodabljajo varnostne konfiguracije omrežij in sistemov.
- Imajo implementirane rešitve za zaščito pred DDoS napadi (v primeru, da ima izvajalec v vzdrževanju tudi infrastrukturo-strežnik).
- Uporabljajo tehnologije za preprečevanje izgube podatkov (DLP).
- Redno ocenjujejo in izboljšujejo varnostne politike.
- Zagotavljajo, da so vsi varnostni dogodki ustrezno evidentirani in obravnavani.
- Izdelajo in vzdržujejo načrt za odzivanje na kibernetske incidente. V primeru, da načrta nimajo vzpostavljenega ga morajo obvezno izdelati.
- Izvajalec postavi sistem v načinu visoke razpoložljivosti, skladno z SLA (odvisno od kritičnosti informacijskega sistema).
- Zagotavljati mora ustrezno fizično in logično varnost podatkovnih centrov (v primeru, da ima izvajalec v vzdrževanju tudi infrastrukturo-strežnik).
- Izvajalec izdela načrt obnove sistema in ga redno testira in posodablja (Standard Operating Procedures). Izvedba preizkusa preklopa skupaj z vsemi deležniki (UKCL, Skrbniki infrastrukture, Skrbniki aplikacije).
- Izvajalec mora vsaj 1x letno predati poročilo varnostnega preverjanja aplikacije, ki vključuje vdorno testiranje in varnostno preverjanje;
- Razvita programska oprema mora biti testirana skladno z najnovejšimi OWASP priporočili. OWASP Open Web Application Security Project) testiranje je skupina vizualizacij in

postopkov za testiranje varnosti spletnih aplikacij in web servisov, ki jih je razvil odprtokodni skupni tok OWASP. Cilj temelji na uporabi različnih testnih metodologij za katalogizacijo in verifikacijo varnosti aplikacije;
- Odpravljanje visokih in srednjih ranljivosti se morajo sproti odpravljati najkasneje 6 mesecev od začetka pogodbe;
- Naročnik si pridružuje pravico do naročila zunanjega izvajalca, ki bo varnostno preveril sistem. Izvajalec je zavezan da bo odpravil vse zaznane ranljivosti;

2. Tehnične smernice, katerim je potrebno slediti pri implementaciji kateregakoli novega spletnega klienta (vmesnika) na UKCL

Tehnične smernice so:

- **Odziven design (Responsive design)**
  Prikaz spletne aplikacije se mora avtomatično prilagoditi različnim formatom zaslonov oz. povečevanju manjšanju okna kjer se vsebina izrisuje. npr. To lahko pomeni zlaganje elementov enega pod drugim v primeru ožanja po horizontali oz. skrivanje določenih elementov.

- **Uporaba sodobnih JavaScript ogrodij za razvoj spletnih aplikacij**
  Sodobna odprtokodna in razširjena orodja, ki se danes uporabljajo in omogočajo izgradnjo dinamičnih, interaktivnih spletnih aplikacij so React, Vue.js.

- **Napredne spletne aplikacije (Progressive Web App - PWA)**
  Aplikacija mora po potrebi omogočati offline način delovanja, komunikacijo v realnem času npr. signalR in podpirati native-app like uporabniško izkušnjo. Npr. namestitev kot samostojna (offline ali online) aplikacija na mobilni napravi.

- **Upravljanje stanja (State management) znotraj spletnih aplikacij**
  Uporaba orodij/knjižnic kot so Redux, Vuex, Pinia za upravljanje stanja znotraj spletnih aplikacij omogoča dinamično uporabniško interakcijo in konsistentnost prikaza podatkov skozi različne dele aplikacije.

- **Uporaba sodobnih standardov in priporočil za zagotavljanje varnosti**
  Uporaba HTTPS. Definiranje Content Security Policies (definira kaj so viri skript in ostalih resursov, ki se izvajajo v spletni aplikaciji), ki preprečuje določene tipe napadov kot so podtikanje skript. Uporaba sodobnih standardnih načinov za avtentikacijo kot je Oauth2/OpenID. Uporaba glavnih uveljavljenih standardov v zdravstvu (Health standardov), kot je npr. HL7, IHE, FHIR,…

3. Smernice za implementacijo in nalaganje (deploy) novih servisov

Smernica za implementacijo so:

- **Modularna mikroservisna arhitektura**

Servisi morajo biti razviti na način, ki omogoča neodvisnost, enostavno nalaganje, skalabilnost in medsebojno povezljivost.
Modularen pristop omogoča organsko rast sistema in enostavno dodajanje novih funkcionalnosti. Prav tako omogoča izolirano zamenjavo oz. nadgradnjo posameznih modulov z minimalnim vplivom na delovanje celotnega sistema.

- **Standardni protokoli za komunikacijo med posameznimi moduli**
  Medsebojna komunikacija med servisi mora potekati preko standardnih in uveljavljenih protokolov kot so REST HTTP in GRPC, AMQP. Komunikacija servisov naj bo zasnovana kot (oz. odvisno od vsebine procesa naj omogoča) »event driven« (dogodkovni) pristop. Preostali servisi se lahko naročijo na določene dogodke sistema in na osnovi tega vodijo svoj proces naprej.

- **Uporaba podatkovnega vodila (Service bus) za integracijo in obveščanje o dogodkih med posameznimi servisi**
  Z uporabo podatkovnih vodil, kot so RabbitMQ, Kafka in »event driven« prisotna zmanjšamo odvisnost (direktne integracije) med posameznimi servisi, omogočimo hitrejši tok informacij (PUSH pristop) in razbremenimo sistem. Prav tako omogočimo dostop do informacij vsem udeležencem, ki jih potrebujejo brez potrebe po še eni dodatni integraciji med dvema servisoma.

- **Uporaba konteinerjev kot načina za razvoj in deplojment servisov**
  Nalaganje servisov v okviru konteinerjev omogoča konsistentnost obnašanje aplikacije čez različna okolja. Konteinerji bolj učinkovito uporabljajo resurse kot običajne virtualne mašine omogočajo ob doseganju enak izolacije procesov.

- **Monitoriranje servisov/telemetrija/Observability**
  Servisi morajo podpirati standardne mehanizme obveščanja o svojem trenutnem statusu. Standardni protokoli kot je OpenTelemetry omogočajo zajem podatkov o logih, metrikah in sledeh (tracing) preko katerih lahko nadziramo delovanje sistema kot celote, odzivnost, prepustnost sistema, ugotavljamo ozka grla in morebitne napake.
  Vsak servis mora imeti implementiran način za preverjanje zdravstvenega stanja (Health check), ki pomeni ali je sistem operativen ali ne. Z avtomatskimi mehanizmi nezdrave servise odstranimo iz delovanja in jih nadomestimo z zdravimi.

4. Neprekinjeno poslovanje in obvladovanje tveganj vezano na informacijski sistem

Informacijski sistem, ki je identificiran kot kritični sistem in je del »kritične IT infrastrukture« v UKCL je pomembno obvladovanje tveganj v primeru izpada informacijskega sistema.

Zahtevana stopnja delovanja SLA za kritične sisteme je razpoložljivost 99,9%.

Za kritične sisteme/servise je potrebno zagotoviti spremljanje (monitoriranje) v avtomatičnem načinu 24/7 z aktivnimi mehanizmi obveščanja (mail, SMS,…).

Zahteve in smernice, ki jih mora zagotavljati izvajalec za vzpostavitev sistema neprekinjenega poslovanja (Business Continuity) in obvladovanja tveganj (Risk Management) za informacijski sistem. Namen je zagotoviti, da organizacija lahko nadaljuje svoje ključne poslovne funkcije tudi v primeru motenj.

Za zagotovitev neprekinjenega poslovanja in varnosti informacijskega sistema mora izvajalec skrbeti za načrtovanje v zvezi z zagotavljanjem neprekinjenega poslovanja in obvladovanja tveganj (Recovery Time Objective – RTO):

- **Avtomatizirane skripte**

  Uporaba avtomatiziranih skript za namestitev in konfiguracijo infrastrukture. Zagotovitev konsistentnosti vzpostavitve celotnega produkcijskega in testnega okolja.

- **Uravnoteženje obremenitve (Load Balancing)**

  Razporeditev prometa med več instancami zabojnikov za zagotavljanje, da noben servis ni preobremenjen in da okvara enega ne vpliva na celoten sistem.

- **Konfiguracijske datoteke**

  Namestitvene skripte in ostale konfiguracijske datoteke se hranijo z orodji za upravljanje s kodo, tako da je vedno na voljo zadnja verzijo potrebnih konfiguracij. Omogočati mora tudi vpogled v zgodovino sprememb konfiguracije.

- **Obveščanje in spremljanje (Monitoring)**

  Monitoring sistema, ki na nivoju vsakega servisa, ki se izvaja v zabojniku sporoča svoje zdravstveno stanje (Health Check). V primeru nedelujočega zabojnika so implementirani mehanizmi, ki nezdrav zabojnik avtomatično resetirajo. Samodejno obveščanje skrbnikov o težavah za hitro ukrepanje.

- **Failover sistemi (Cluster sistem)**

  Servisi sistem se morajo izvajajo v zabojnikih z več instancami, kar pomeni da obstaja redundanca, ki tudi ob izpadu ene instance zagotavlja neprekinjeno delovanje.

- **Neprekinjena zaščita podatkov (Continuous Data Protection - CDP)**

  Omogočati mora sprotno varnostno kopiranje podatkov, kar omogoča obnovitev podatkov do točno določenega časa.

- **Posodabljanje**

  Redno posodabljanje in nadgradnje aplikativne programske opreme.

- **Povezljivost, robustnost in dosegljivost sistema**

  Glede na kritičnost mora imeti sistem/servis določeno stopnjo redundance. Uporaba predlaganih tehnologij, kot so zabojniki (tehnološke smernice), omogoča enostavno umestitev in integracijo teh servisov z orodji za doseganje visoke razpoložljivosti, kot so Kubernetes, Docker Swarm, Service Fabrics.

Izvajalec mora v primeru kritičnega izpada vzpostaviti informacijski sistem (Recovery Point Objective – RPO) in obnoviti podatke v času izpada

V primeru kritičnega izpada informacijskega sistema UKCL se čas potreben za ponovno vzpostavitev informacijskega sistema opredeljen v SLA.
Skupni čas ponovne vzpostavitve delovanja celotnega sistema odvisen od časa ponovne vzpostavitve in delovanja vseh teh kritičnih delov, ki so v integraciji z drugimi izvajalci v okolju UKCL.

5. Lokacija podatkov

Vsi podatki za produkcijska okolja morajo biti locirani na strežnikih v profesionalnem podatkovnem centru (angl. »Data center«) v UKC Ljubljana. Vse povezave med strežniki (testni in produkcijski) in izvajalcem morajo biti enkriptirane in preko namenskih VPN-ov. V primeru, da je lokacija podatkov in aplikacij izven UKC Ljubljana in se izvajajo servisi v omrežje UKC Ljubljana morajo biti povezave ustrezno zaščitene.

6. Rok hrambe

Rok hrambe mora biti nastavljiv za vsak poslovni proces ločeno.

7. Podpora in vzdrževanje

Izvajalec mora vzdrževati in izboljševati uporabo programa ter izpolnjevati nove zahteve funkcionalnosti, ki jih zahteva naročnik.

Garancijska doba za odpravo napak za storitve, opravljene v okviru dopolnilnega vzdrževanja, ki posegajo v področje funkcionalnosti sistema, je 12 mesecev od naročnikove potrditve izvedbe naročila. Odpravljene napake storitev oziroma na storitvah, ki so opravljene v okviru dopolnilnega vzdrževanja, so po preteku 12 mesecev od naročnikove potrditve izvedbe naročila predmet osnovnega vzdrževanja sistema.

Izvajalec je dolžan dopustiti in omogočiti naročniku učinkovit nadzor nad kvaliteto opravljenih storitev. Naročnik ima pravico v času veljavnosti te pogodbe angažirati strokovnjake - poznavalce tehnologije in revizorje informacijskih sistemov, za presojo kakovosti opravljenih storitev (kakovost rešitev, ustreznost procesa izdelave, testiranja in dobave rešitev, ustreznost rešitev z vidika varovanja podatkov). V primeru takšnih presoj je izvajalec dolžan sodelovati s temi strokovnjaki in jim omogočiti dostop do tehnične dokumentacije in izvorne kode.

Naročnik je dolžan izvedbo presoje napovedati najmanj 8 dni pred presojo. V kolikor se med presojo ugotovijo neskladnosti, stroške revizije krije v celoti izvajalec.

Naročnik uporablja za podporo in upravljanje ITSM procesov (storitveni zahtevki, incidenti, problemi, spremembe, SLA in upravljanje IT sredstev) aplikacijo za upravljanje storitev IBM Maximo Control Desk (Maximo IT). Naročnik zahteva, da izvajalec redno beleži in rešuje vse zahtevke, incidente, spremembe ter ostale procese in mesečno poroča o dejansko opravljenem delu, njegovi vsebini in obsegu v naročnikovi aplikaciji IBM Maximo Control Desk (Maximo IT). V primeru, da zunanji izvajalec že ima vzpostavljen lasten sistem za beleženje, mora izvajalec na lastne stroške zagotoviti integracijo z IBM Maximo Control Desk (Maximo IT).

8. Odprava napak (SLA - Service level agreement)

V okviru osnovnega vzdrževanja mora izvajalec zagotavljati odpravo napak. Napaka definirata kot nedelovanje informacijskega sistema oziroma delovanje, ki ni v skladu z zahtevanimi specifikacijami.

Napake se delijo glede na resnost, od česar je odvisna tudi hitrost oziroma nujnost odprave, in sicer:

- **Kritična napaka:**
  - uporaba sistema je v celoti onemogočena in je s tem onemogočeno izvajanje procesov,
  - ni možnosti obhoda napake.

- **Zelo resna napaka:**
  - uporaba sistema je za nekatere sklope onemogočena kar povzroča težave pri izvajanju procesov,
  - obstaja postopek obhoda napake.

- **Srednje resna napaka:**
  - uporaba sistema oziroma posameznih sklopov je mogoča, vendar otežena, proces se lahko kljub temu izvaja,
  - obstaja postopek za izogibanje težavi.

- **Napake z nizko pomembnostjo:**
  - sistem deluje, problem predstavlja manjšo neprijetnost uporabniku, če je povezano z napako v delovanju.

Odzivni čas je čas, ki preteče od prejema prijave napake, do trenutka, ko izvajalec začne z odpravljanjem napake. Čas za odpravo napake je tisti čas, ki preteče od prejema zahteve za odpravo napake, do takrat, ko je izvajalec odpravil napako. Odzivni čas na prijavo napak in čas za odpravo napake je odvisen od tipa napake.

Odzivni čas za prijavo napak oziroma incidentov v rednem delovnem času (ponedeljek do petek med 8 in 16 uro):

Tip napake	**Odzivni čas**	***Čas za odpravo napake**
Kritična napaka	1 ura	**4 ure
Zelo resna napaka	4 ure	8 ur
Srednje resna napaka	8 ur	24 ur
Napake z nizko pomembnostjo	12 ur	48 ur

**Nenehno poskušanje oziroma 4 ure

Odzivni čas za prijavo napak oziroma incidentov in čas za odpravo napak oziroma incidentov izven delovnega časa:
- ponedeljek do petek med 16 in 8 uro zjutraj,
- sobota in nedelja pa je 24/7.

Tip napake	**Odzivni čas**	***Čas za odpravo napake**
Kritična napaka	1 ura	**4 ure
Zelo resna napaka	4 ure	8 ur
Srednje resna napaka	8 ur	24 ur
Napake z nizko pomembnostjo	12 ur	48 ur

**Nenehno poskušanje oziroma 4 ure

Nenehno poizkušanje razen v primerih, ko je za napako potrebna zamenjava dela strojne opreme ali popravek sistemske opreme in je čas odprave napake pogodbeno določen oziroma zagotovljen s strani

principala (IBM,…).

9. Ukrepanje in rezultati

Ko izvajalec prejme prijavo o napaki, potrdi status in vsebino zadevne napake v "odzivnem času" (kot je opredeljen v nadaljevanju). Izvajalec opravi oceno zahtevnosti posamezne zahteve. Po potrebi lahko izvajalec skupaj z naročnikom oceni zapletenost posamezne zahteve in se odloči, kako nadaljevati. Izvajalec obvesti naročnika o predvidenem datumu odprave napake in o potrebnih dejavnostih, ki jih je treba pri tem izvesti.

Izvajalec se odzove z akcijskim načrtom, namenjenim odpravi napake. Dejanski zahtevani odzivni čas je odvisen od resnosti napake in je naveden v zgornji tabeli.

Odprava napake lahko pomeni tudi implementacija alternativne začasne rešitve.

Po odpravi napake izvajalec o njeni odpravi obvesti naročnika oziroma se navedeno uredi v okviru ustrezne informacijske rešitve obveščanja o napaki.

V primeru, da izvajalec prekorači odzivni čas ali čas za odpravo napake, so posledice opredeljene v pogodbi.

10. Poročilo o delovanju platforme in odpravi napak

Izvajalec je dolžan naročniku predložiti poročilo o napaki, iz katerega bo razviden vzrok nastanka napake, predviden čas odprave napake ter obrazložitev napake. Poročilo je izvajalec dolžan v primeru kritičnih napak predložiti nemudoma po prijavi napake oziroma najkasneje v roku 24 ure po prijavi. V primeru nekritičnih napak je izvajalec dolžan poročilo predložiti naročniku najkasneje v roku 24 ur od začetka odpravljanja napake. Če izvajalec oceni, da bo odprava kritične napake trajala več kot štiri ure, mora o tem obvesti naročnika.

Točka 1: Osnovno vzdrževanje in podpora uporabnikom (24/7) za laboratorijski informacijski sistem (LIS) za obdobje 48 mesecev, ki zajema naslednje module:

- Laboratorijski informacijski sistem LIS (LIS.EXE);
- Prenos podatkov med instrumenti (DATATR.EXE);
- Prenos podatkov iz analizatorjev v LIS (UNIV_datatr.EXE);
- Arhiviranje podatkov (ARHIVAR.EXE);
- Prenos naročil in izvidov med oddelki in laboratoriji (MAINTRAN.EXE) – povezava s programi Hipokrat, Birpis21/ISoz21 in Clinical;
- Prenos izvidov in obračunskih podatkov (BASETRANS.EXE) - povezava z programom BIS;

- Prenos obračunskih podatkov (ERAC.EXE)- povezava s programom Webpis;
- Prenos podatkov za zunanje naročnike (MGWCOMMUN.EXE) – povezava s portalom Medgetway (Infonet d.o.o.);
- Internetne komunikacije z zunanjimi naročniki (LABBHTTP.EXE);
- Povezava POCT analizatorjev (ISTAT - InfoHQ, ABL in Emerald);
- Prenos obračunskih podatkov interne realizacije v Power BI;
- Prenos podatkov in laboratorijskih izvidov v CDR, CDR TRANSFER.exe;
- Prenos laboratorijskih izvidov v CRPP.

Laboratorijski informacijski sistem (LIS) se trenutno uporablja v naslednjih laboratorijih UKC Ljubljana:

- Klinični inštitut za klinično kemijo in biokemijo;
- Interna klinika, Klinični oddelek za žilne bolezni, Laboratorij za hemostazo in aterotrombozo;
- Interna klinika, Klinični oddelek za endokrinologijo, diabetes in presnovne bolezni, Oddelek za ambulantno in diabetološko dejavnost;
- Interna klinika. Klinični oddelek za revmatologijo, Laboratorij za imunologijo revmatizma;
- Interna klinika, Klinični oddelek za hematologijo, Laboratorij za hemostazo in citološki laboratorij;
- Nevrološka klinika, Klinični oddelek za bolezni živčevja, Laboratorij za likvorsko diagnostiko;
- Pediatrična klinika, Klinični inštitut za specialno laboratorijsko diagnostiko;
- Dermatovenerološka klinika, Mikološki laboratorij, Alergološki laboratorij;
- Klinika za nuklearno medicino, Oddelek za radiokemijo in radiofarmacijo;
- Klinični inštitut za genomsko medicino, Laboratoriji.

Storitve osnovnega vzdrževanja in podpore uporabnikom (24/7) za laboratorijski informacijski sistem (LIS) obsegajo:

- Osnovno vzdrževanje, ki obsega:
  - Zagotavljanje operabilnosti informacijskega sistema na ravni funkcionalnosti iz strokovnih zahtev.
  - Uporaba skupnih šifrantov. Naročnik zagotovi šifrante, izvajalec pa mora zagotoviti ažuriranje teh šifrantov v laboratorijski informacijski sistem (LIS).
  - Določanje uporabniških pravic v skladu z dogovorjenimi pooblastili in dostopnimi pravicami. Izvajalec mora omogočati pooblaščenim osebam naročnika tudi dostop do revizijskih sledi.
  - Odpravljanje skritih napak na aplikativni programski opremi.
  - Preventivni trimesečni (3) pregledi delovanja sistemske programske opreme (operacijski sistemi, sistemi za upravljanje z zbirkami podatkov, sistemska programska oprema na aplikativnih strežnikih, sistemska programska oprema za izvajanje komunikacij s podsistemi v okolju).
  - Preventivni trimesečni (3) pregledi konsistentnosti podatkovnih zbirk.
  - Preventivni trimesečni (3) pregledi odzivnosti sistema (tuning).
  - Izvajanje ukrepov za zagotavljaje konsistentnosti in odzivnosti sistema (nastavitve v sistemski programski opremi in izboljšave v aplikativni programski opremi).
  - Nameščanje novih verzij aplikativne programske opreme.
  - Pisno obveščanje naročnika o novih verzijah oz. spremembah na verzijah, ter uskladitev termina nameščanja novih verzij.

- Namestitev, uvedba in uporaba obstoječih modulov na dodatnih ali novih lokacijah v UKC Ljubljana.
- Izvajalec storitev je dolžan ob izstavitvi računa za določen mesec izdati pisno specifikacijo o izvedenih storitvah osnovnega vzdrževanja in storitvah podpore uporabnikom.
- Spremljanje tehnoloških novosti, priprava in posredovanje predlogov za izboljšave delovanja sistema, ki ni predmet osnovnega vzdrževanja.
- Prilagoditev modulov zakonskim in/ali regulatornim spremembam ter prilagoditev modulov standardom v laboratorijski medicini.
- Izvajanje validacij nadgradenj sistema s pisnim poročilom.

- Podpora uporabnikom 24 ur na dan vse dni v tednu (24/7), ki vključuje tudi svetovanje in pomoč pri uporabi posameznih modulov.

Točka 2: Dopolnilno vzdrževanje laboratorijskega informacijskega sistema (LIS) za obdobje 48 mesecev

Dopolnilno vzdrževanje laboratorijskega informacijskega sistema (LIS) je opredeljeno v urah, ki so potrebne za uresničitev zahtev naročnika, ki niso del osnovnega vzdrževanja. Storitve dopolnilnega vzdrževanja so omejene v obsegu **4.000 ur za obdobje 48 mesecev.**

Storitve dopolnilnega vzdrževanja se izvajajo na osnovi pisnega zahtevka naročnika, ki ga zastopa pooblaščena oseba (strokovni skrbnik pogodbe ali v protokolu dela na strani naročnika določen koordinator laboratorijskega informacijskega sistema (LIS)) in zajema vsebino, obseg storitve in pričakovane roke za izvedbo. Izvajalec mora izdati ponudbo z ocenjenim obsegom ur in rokom za izvedbo v 8 delovnih dneh od prejetja pismenega zahtevka. Ponudbo mora pooblaščena oseba naročnika potrditi.
Izvedene storitve dopolnilnega vzdrževanja se potrdijo s podpisom primopredajnega zapisnika.

Ure v okviru dopolnilnega vzdrževanja so namenjene:
- Razvoju novih funkcionalnosti posameznih modulov na zahtevo naročnika, ki niso zakonske in/ali regulatorne narave.
- Prilagoditve posameznih modulov zaradi uvedbe laboratorijskega informacijskega sistema (LIS) na drugih lokacijah v UKC Ljubljana.
- Uresničitev povezave z drugimi informacijskimi rešitvami na zahtevo naročnika, kadar je potrebno razviti nov komunikacijski protokol.
- Uresničitev sprememb protokolov povezav z drugimi informacijskimi sistemi.
- Priklop novih POCT analizatorjev v UKC Ljubljana, v laboratorijski informacijski sistem (LIS).
- Druge storitve na zahtevo naročnika.

Garancija za vse storitve razvoja novih funkcionalnosti je 12 mesecev od podpisanega primopredajnega zapisnika za izvedene storitve. Po preteku 12 mesecev od podpisanega primopredajnega zapisnika za izvedene storitve je odprava napak predmet osnovnega vzdrževanja.

1. **Zahteve naročnika:**
   - Ponudnik Laboratorijskega informacijskega sistema mora imeti vsaj 4 reference, v drugih bolnišničnih ustanovah po Sloveniji.