

TEHNIČNE IN NEUNKCIONALNE SPECIFIKACIJE ZA  
ČPZM  
(MODUL ZA ČEZMEJNE PRENOSNE ZMOGLJIVOSTI)

Ljubljana, 8. 05. 2024

## Vsebina

REVIZIJA DOKUMENTA.....	Error! Bookmark not defined.
1 UVOD .....	4
1.1 Kratice in definicije.....	4
2 Popis zahtev.....	5
2.1 Splošne varnostne zahteve .....	5
2.2 Splošne zahteve uporabe infrastrukturnih strežniških virov .....	6
2.3 Uporabnost .....	7
2.4 Razpoložljivost.....	8
2.5 Zanesljivost .....	8
2.6 Zmogljivost .....	9
2.7 Skalabilnost.....	9
2.8 Komunikacijske zahteve .....	10
2.9 Vzdrževanje in upravljanje s popravki/spremembami .....	12
2.10 Licenciranje in izvorna koda .....	13
2.11 Produktijsko, , testno, razvojno okolje.....	13
2.12 Zakonske zahteve in interna pravila .....	14
2.13 Projekt za izvedbo (PZI) in Projekt izvedenih del (PID) .....	14

## Kazalo slik

Slika 2–1 Umestitev IS ICMM v Elesovo okolje .....	11
--	----

## Kazalo tabel

Nobenega vnosa v kazalo slik ni bilo mogoče najti.

# 1 UVOD

ELES posreduje informacije za upravljanje s prenosnimi zmogljivostmi v okviru procesa ID čezmejne izmenjave energije na skupno platformo (tj. XBID). Dodatno pa bo v okviru čezmejne izmenjave izravnalne energije iz naslova avtomatskega procesa za povrnitev frekvenca (aFRR) in ročnega procesa za povrnitev frekvenca (mFRR) moral vsak operater prenosnega sistema (OPS) zagotoviti podatke o razpoložljivih čezmejnih prenosnih kapacitetah in jih posredovati na platformo za skupno upravljanje s prenosnimi zmogljivostmi (CMM oz. Capacity Management Module), ta pa bo nato skrbela za določitev in posredovanje omejitev na posamezne izravnalne platforme (tj. MARI in PICASSO/IGCC). Ker bo OPS s strani izravnalnih platform ves čas prejemal povratne informacije o porabljenih prenosnih zmogljivosti, bo lahko sproti preverjal izračune CMM orodja in v primeru njegovega nedelovanja (t.i. »fall-back« postopka) sam posredoval podatke na posamezne platforme. V ta namen bo ELES potreboval interno orodje, t.i. ICMM (Internal CMM), ki bo na eni strani pridobil vse ustrezne podatke, kot so NTC, AAC ter dodatne omejitve, ki jih bo podal operater, ter jih ustrezno obdelal, kjer bo to treba, in jih posredoval CMM in/ali posamezno platformo. V okviru ICMM bo proces določanja prenosnih zmogljivosti za ID poteka za obdobje od zaključka D-1 trgovanja (D-9h) do zaključka ID trgovanja (H-60 min), proces določevanja prenosnih zmogljivosti za izravnalne platforme pa bo potekal za obdobje med zaključkom ID trgovanja (H-60 min) in zaključkom vsakega 15 minutnega intervala (QH).

Namen dokumenta je predstaviti opis delovanja, določitev izračunov in integracijo orodja v Elesove sisteme. Na koncu so predstavljene funkcionalne zahteve.

## 1.1 Kratice in definicije

CMM (Capacity Management Module) – skupna evropska platforma za izmenjavo in preračun prenosnih kapacitet

ECP/EDX – Electronic Communication Protocol/Energy Data Exchange platform

MARI – Manually Activated Reserves Initiative

OPS (TSO) – operater prenosnega sistema

PS – Podatkovno skladišče

PICASSO – Platform for the International Coordination of Automated Frequency Restoration and Stable System Operation

SIDC (XBID) – Single intraday market coupling

SS (Scheduling System) – sistem za najavo voznih redov

XBID (SIDC) – Single intraday market coupling

RTO – Recovery Time Objective – čas do povrnitve storitve po katastrofi

RPO – Recovery Point Objective – čas izgube podatkov ob katastrofi

MS – Microsoft

AD – Active Directory – Aktivni imnenik

AMQP – Advanced Message Queue Protocol

SFTP – Seceure File Tranfer Protocol

SMB – Server Message Block

API – Application Programming Interface

RBAC – Role-based access control

## 2 Popis zahtev

### 2.1 Splošne varnostne zahteve

- Uporabniški vmesnik mora biti izveden kot spletna aplikacija; objavljena mora biti samo preko varne povezave (https).
- Uporabniški vmesnik mora delovati na standardnih spletnih brskalnikih brez namestitve vtičnikov ipd. (vsaj MS Edge).
- Sistem mora beležiti dnevniške zapise in revizijske sledi.
- Sistem mora beležiti in omogočati pošiljanje dnevniških zapisov in revizijskih sledi v obliki syslog. Zahtevana je izvedba integracije s SIEM sistemom ELES.
- Prijava v storitev (avtentikacija) mora potekati na način, ki onemogoča nepooblaščno razkritje ali uporabo avtentikacijskih podatkov.
- Vse povezave, ki se uporabljajo za izmenjavo podatkov znotraj ELES omrežja morajo biti šifrirane.
- Šifriranje podatkov in komunikacij mora biti izvedeno s sodobnimi močnimi šifrirnimi algoritmi in metodami. Uporaba šibkih šifrirnih algoritmov in metod ne sme biti mogoča.
- Avtentikacijski podatki se ne smejo prenašati ali biti shranjeni v nešifrirani obliki.
- Omogočeno in popisano mora biti spreminjanje gesel vseh računov s privilegiranimi pravicami.
- Uporabniški vmesnik mora podpirati uporabo sistema enkratne prijave (SSO), MS AD.
- Sistem mora podpirati standardne vmesnike za integracijo z MFA (multifaktorska avtentikacija) sistemi.

- Sistem mora podpirati standardne vmesnike za integracijo s PAM (upravljanje privilegiranih računov) sistemi, za katero aktualna navodila zagotovi naročnik ob pripravi PZI,
- Sistem mora podpirati standardne vmesnike za integracijo z IM (upravljanje z identitetami) sistemi.
- Zahtevana je izvedba ustrezno globoke integracije z IM sistemom ELES, za katero aktualna navodila zagotovi naročnik ob pripravi PZI,
- Zahtevana je vključitev novega SW/HW v centralne nadzorne sisteme PITK, za katero aktualna navodila zagotovi naročnik ob pripravi PZI,
- Zahtevano je upravljanje dostopov na podlagi vlog (RBAC) novega IS ICMM Eles, ki jih uporabniki/administratorji sistema lahko upravljajo samostojno. Pripadajoče lokalne vloge IS ICMM morajo biti dostopne in dodeljene članom uporabniških skupin MS AD aktivnega imenika.

## 2.2 Splošne zahteve uporabe infrastrukturnih strežniških virov

- Sistem mora delovati na strežniku Microsoft Windows Server 2022 ali novejši.
- Sistem mora za hranjenje podatkov uporabljati podatkovno bazo Microsoft SQL 2019. Naslov za povezovanje na MS SQL operativno podatkovno bazo IS ICMM je enovit in sledi standardnem poimenovanju pri uporabi v družbi Eles – ICMMDBP, ICMMDBpP, ICMMDBT, Hranjenje vsebin v izmenjavi je hrani v relacijski podatkovni bazi (v nadaljevanju RDB) »DwVozniRedi«, medtem, ko je za operativne potrebe IS ICMM na voljo RDB »ICMMdb«. Varovanje podatkov pred izgubo in zagotavljanje visoke razpoložljivosti zagotavlja naročnik z uporabo lastnih tehnologij.
- Uporabnik/Naročnik bo opredelil zahteve po pogostosti (časovni interval) varnostnega kopiranja in čas hranjenja varnostnih kopij, ki jo mora izvajalec tudi upoštevati. Sistem mora podpirati izvedbo varnostnega kopiranja s produktom Veeam Backup & Recovery, ki bo temeljilo na internih pravilnikih naročnika.
- Uporabnik/Naročnik mora oblikovati oceno potrebnega diskovnega prostora – inicialna zahteva ter predvideni letni prirast.
- Uporabnik/Naročnik bo opredelil zahteve po pogostosti (časovni interval) arhiviranja podatkov, medtem, ko mora IS ICMM omogočati delitev in oblikovanje arhivskih podatkov, kar bo po potrebi definirano pri oblikovanju vsebin PZI,
- IS ICMM mora podpirati delovanje na rešitvi za virtualizacijo vmWare 7.0. ali višje.
- Uporabniški del IS ICMM – spletni uporabniški vmesnik, mora biti izveden na spletnem strežniku IIS 10.0 (ali novejši),
- IS ICMM mora zagotoviti ločevanje upravljalškega/administrativnega in uporabniškega vmesnika.

## 2.3 Uporabnost

IS ICMM mora biti zasnovana kot sodobna rešitev, ki omogoča uporabniku na čim bolj enostaven, učinkovit in prijazen način izvesti vse poslovne procese predvidene za zagotavljanje zakonskih zahtev. Rešitev mora omogočati standardizacijo in avtomatizacijo procesov povsod tam, kjer je to mogoče in smotrno.

IS ICMM se mora vidno odzivati na uporabnikove akcije. Vsaka akcija povzroči vidno (logično in prepoznavno) spremembo na uporabniškem vmesniku. Ko orodje ni odzivno, uporabniku to vidno prikaže (sprememba kurzorja, prikaz poteka postopka, proženje dogodka s prikazom dogodka v novem oknu »pop-up«, zapis v dnevnik dogodkov in podobno).

Informacijska rešitev IS ICMM mora zagotavljati enostavno (intuitivno) uporabo funkcionalnosti. Kjerkoli je pričakovana takojšnja interakcija z uporabnikom, mora rešitev uporabniku ponuditi takojšen odziv in biti čim bolj prilagojena učinkoviti uporabi (čim manjše število korakov za izvedbo določenega postopka, čim hitrejši dostop do kakovostnih informacij, ...).

Ključna zahteva glede funkcionalnosti rešitve je enostavnost uporabe in hitra odzivnost.

Uporabniški vmesnik mora slediti naslednjim smernicam:

- ustrezno segmentiranje in zaporedje vnosnih polj uporabniškega vmesnika, ki uporabniku dajeta jasno informacijo glede statusa in procesa zajema podatkov,
- kontrola pravilnosti in veljavnosti vpisanih podatkov, kjer je to mogoče (ali z znanim algoritmom ali s preverjanjem podatkov v zunanem viru),
- uporaba pred izpolnjevanja ali izbire možnih vrednosti, kjer je to le mogoče,
- izvedba posameznih aktivnosti v čim manj korakih (optimizirani procesi v uporabniškem vmesniku programske opreme),
- vnos podatkov na enem mestu, ponovna uporaba podatkov, ki so že zajeti v rešitev ali v drugih povezanih informacijskih sistemih, s katerimi je zagotovljena izmenjava podatkov. Enkratni zajem oziroma vnos podatkov v šifrante ter avtomatični prenos teh podatkov v vse module rešitve, ki uporabljajo te šifrante,
- komunikacija z uporabnikom, kjer so na enoten način uporabljeni elementi, kot so sporočila o napakah, obvestila o napredku obdelave in podobno,
- elementi (grafični gradniki) morajo biti oblikovani tako, da v različnih brskalnikih in operacijskih sistemih omogočajo podoben videz in enakovredno funkcionalnost,
- varno skupno delo več uporabnikov na enem zapisu v smislu skupne rabe (vsebine lahko ureja več uporabnikov hkrati) ali pa možnost vsaj hkratnega ogleda vsebine (pri čemer lahko vsebino ureja le en uporabnik hkrati).

## 2.4 Razpoložljivost

Zagotavlja neprekinjenega poslovanja bo naročnik zagotavljal možnost izvajanja strežnikov na dveh lokacijah z uporabo tehnologij replikacije virtualnih strežnikov z uporabo z vSphere in vSAN – na nivoju vSphere metro gruče. Prav tako je na nivoju MS SQL strežnika zagotovljena replikacija podatkovnih baz in dostopa do njih z uporabo »availability group« na obeh lokacijah podatkovnega centra. Sicer pa se pričakuje od IS ICMM, da sledi zahtevam načrt neprekinjenega poslovanja uporabnikov IS ICMM s sledečimi zahtevami:

- RTO: 1 ura (30min)
- RPO: 1 ure
- V primeru ročnega preklopa, prekop ne sme trajati dlje kot 30 min

Ostale zahteve zagotavljanje primerne razpoložljivosti, bo naročnik po podpisu pogodbe zagotovil iz vsebin lasnih pravilnikov zagotavljanja razpoložljivosti delovanja kritične infrastrukture.

## 2.5 Zanesljivost

Zaradi zahteve po točnosti podatkov, ki se bodo uporabljali v okviru informacijske rešitve, je treba zagotoviti zanesljivost rešitve in njenih podatkov. V tem je treba zagotoviti več varnostnih in kontrolnih mehanizmov, ki bodo omogočali, da so podatki, ki jih uporabnik zahteva, celoviti, točni in odražajo stanje uporabnikovih zahtev.

Zanesljivost delovanja z vidika uporabnika (točke vnosa podatkov) pri vnosih podatkov mora biti zagotovljena z vgrajenimi kontrolami, ki v najvišji meri onemogočajo nepravilen vnos (predvsem morajo biti zagotovljene na nivoju občutljivih podatkov), kot na primer:

- preverjanje dolžin polj, podatkovnega tipa in formata podatka,
- vključitev drugih kontrol (npr. datum začetka del ne sme biti poznejšo kot datum konca del), ki so stvar dogovora in
- odstranjevanje odvečnih presledkov na začetku in koncu polja.

Visoko zanesljivost je treba zagotoviti tudi na nivoju podatkov. V okviru obravnave podatkov mora biti zagotovljeno preverjanje celovitosti podatkov, kjer mora informacijska rešitev zagotoviti, da podatki niso v nobenem trenutku neskladni. V primeru, da pride do napak ali izpada sistema, mora imeti informacijska rešitev zagotovljen mehanizem, ki bo sistemu omogočal prehod v predhodno konsistentno stanje. Prav tako je potrebno v primeru napak zagotavljati mehanizem, ki zagotavlja samodejno zaznavanje napak in proži ustrezne alarme/opozorila.



## 2.6 Zmogljivost

IS ICMM mora zagotavljati:

- nemoteno delovanje in izvajanje funkcionalnosti vsem uporabnikom,
- nemoteno izmenjavo podatkov z drugimi informacijskimi sistemi, kot je opredeljeno v funkcionalnih zahtevah,
- rešitev mora upoštevati, da celotna izmenjava podatkov temelji na Close-to-Real Time in je dopustna latenca pri izmenjavi podatkov je 5000 ms (round trip time (RTT) pošiljatelj-prejemnik),
- v nobenem primeru ob interaktivnem delovanju ne sme programska oprema ponudnika obdelovati podatkov več kot 1 s, po tem, ko je prejela vse podatke iz ostale infrastrukture,
- odzivni čas uporabniškega vmesnika za pregled podatkov in prikaz poročil ter izvajanje obdelav bo natančno opredeljen v okviru priprave PZI. Zahteva naročnika je, da se v okviru priprave PZI opredeli in uskladi tipe vpogleda v podatke in tipe poročil, način njihove priprave (preko spletnega vmesnika, asinhrona priprava poročil v ozadju, predpriprava poročil itd.) ter zahtevane odzivne čase za posamezno kategorijo. Pri tem mora izvajalec zagotoviti takšne odzivne čase za pripravo vpogledov v podatke in poročila, da bodo omogočali zadovoljivo uporabniško izkušnjo,
- posameznih aktivnosti v čim manj korakih, kar zagotavlja optimiziranost procesov v programski rešitvi, vključno z optimalnimi izvajanjem uporabe podatkovne baze (optimalni SQL klici, zaklepanja vsebin, primerna indeksiranja in podobno).

V primeru, da izvajalec zahtevanih odzivnih časov ne more doseči, mora identificirati vzrok, ki ga bo obravnaval skupaj z naročnikom. V primeru, da vzrok za performančne težave ne izvira iz drugih sistemov (ki se npr. odzivajo prepočasi pri izmenjavi podatkov itd.) ali iz informacijskih storitev, za katere je zadolžen naročnik, bo moral izvajalec le-tega odpraviti.

## 2.7 Skalabilnost

Naročnik bo izdelal načrt uporabe in števila uporabnikov in transakcij, kar mora izvajalec upoštevati pri načrtovanju in izdelavi IS ICMM.

Informacijsko rešitev bodo uporabljali večina zaposlenih pri naročniku. Ne glede na to, da bo informacijsko rešitev na začetku uporabljalo fiksno število uporabnikov, se mora upoštevati, da se bo število uporabnikov v prihodnosti povečevalo. Zato mora biti informacijska rešitev prilagojena na način, ki bo omogočal enostavno povečevanje zahteve po številu uporabnikov. Povečevanje števila uporabnikov oziroma drugih odjemalcev v okviru pričakovanih obsegov uporabe informacijske rešitve ne sme vplivati na poslabšanje zmogljivosti sistema.

Izvajalec mora upoštevati načrtovane količine podatkov in primerno oblikovati upravljanje z uporabljenimi podatkovno hrambo, tako na datotečnem prostoru, kot v podatkovnih bazah. Tako mora primerno načrtovati in omogočati izvedbo delitve operativnih in arhivskih vsebin/podatkov, kar se lahko določi ob oblikovanju PZI.

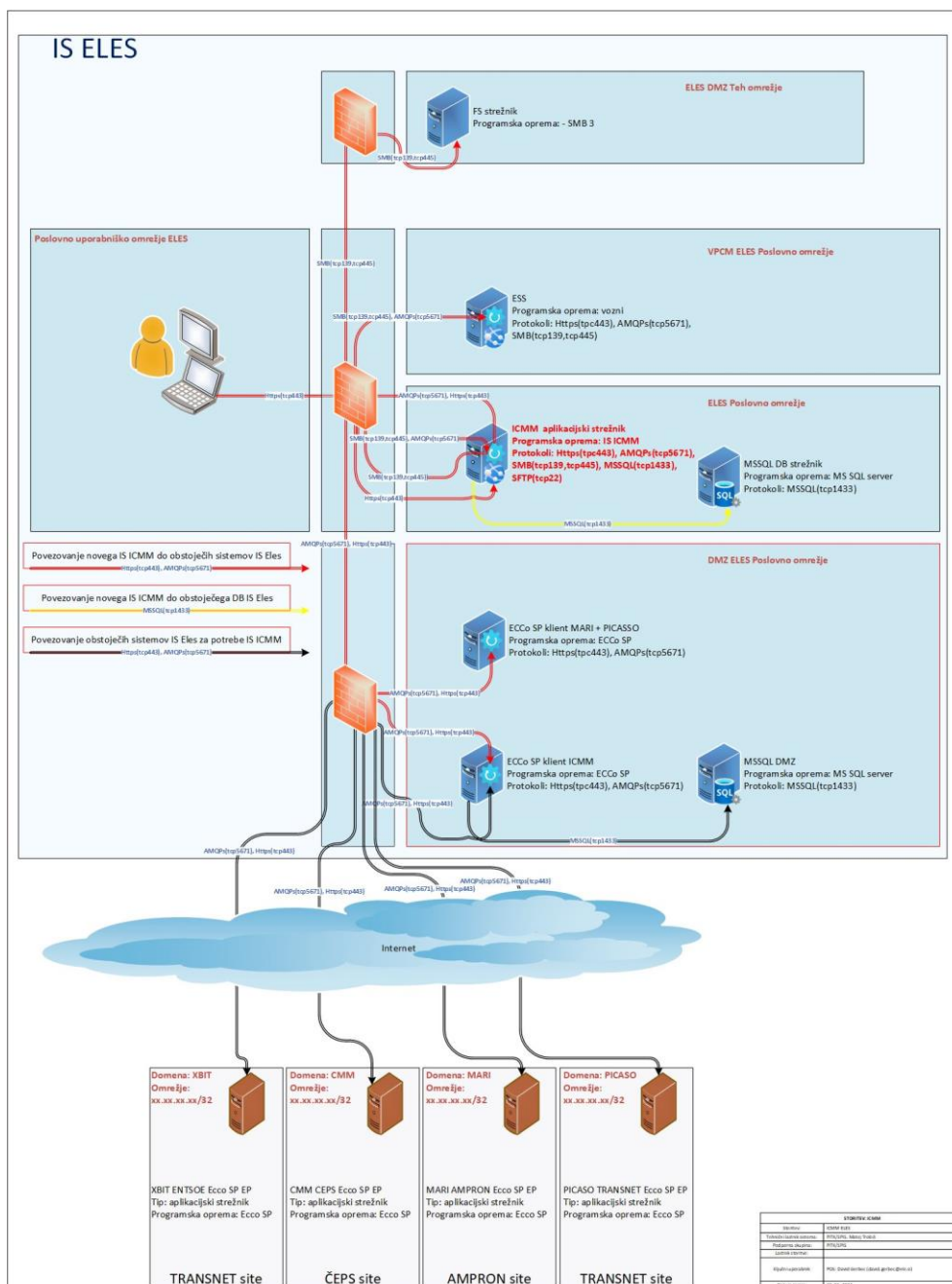
Velikost inicialnih podatkov: 50 GB, Letni prirast: 20 GB

## 2.8 Komunikacijske zahteve

IS ICMM mora biti zasnova tako, da omogoča poljubno uporabniško konfiguracijo izmenjave podatkov z ostalimi deležniki. Posamezna izmenjava podatkov (pravilo izmenjave) bo temeljila na izbiri najmanj sledečih vsebin:

- primarne tehnologije/protokola izmenjave,
  - o določitve poti do deležnika (v odvisnosti od izbrane tehnologije/protokola izmenjave),
  - o določitve uporabnika za dostop do deležnika (v odvisnosti od izbrane tehnologije/protokola izmenjave),
  - o določitve vsebine za izmenjavo (v odvisnosti od izbrane tehnologije/protokola izmenjave),
  - o določitev pogojne ali brezpogojne izmenjave
- sekundarne tehnologije/protokola izmenjave.
  - o določitve poti do deležnika (v odvisnosti od izbrane tehnologije/protokola izmenjave),
  - o določitve uporabnika za dostop do deležnika (v odvisnosti od izbrane tehnologije/protokola izmenjave),
  - o določitve vsebine za izmenjavo (v odvisnosti od izbrane tehnologije/protokola izmenjave),
  - o določitev pogojne ali brezpogojne izmenjave

Načrtovalna visokonivojska umeščenost IS ICMM v IS ELES je predstavljena v Slika 2-1.



Slika 2-1 Umestitev IS ICMM v Elesovo okolje

Podprte/zahtevane tehnologije/protokoli izmenjave so:

- AMQP,
- Web services (SAOP),
- SFTP,
- E-Mail (SMTP),
- SMB,
- FSSP.

Splošne varnostno komunikacijske zahteve:

- Vse povezave, ki se uporabljajo za izmenjavo podatkov preko javnega omrežij, morajo biti šifrirane.
- Spletni vmesnik mora za svoje delovanje uporabljati izključno varne povezave (TLS 1.2 ali TLS 1.3).
- Za izmenjavo podatkov mora aplikacija uporabljati standardne API vmesnike in šifriranje prometa (najmanj TLS 1.2). Omogočena mora biti menjava API ključev.

## 2.9 Vzdrževanje in upravljanje s popravki/spremembami

Redne posodobitve in tehnične izboljšave morajo biti praviloma izvedene tako, da to ne pomeni nedelovanja informacijske rešitve znotraj opredeljenega delovnega časa naročnika. Če se nedelovanju ni mogoče izogniti, mora biti vsaka načrtovana prekinitev delovanja (zaradi npr. nujnih popravkov programske ali strojne opreme, nadgradenj in drugih nujnih del) naročniku sporočena najmanj tri (3) delovne dni pred dejansko izvedbo. V sporočilu mora biti naveden razlog za prekinitev ter čas, v katerem bo izvedena prekinitev. Načrtovana prekinitev delovanja se lahko izvede izven delovnega časa naročnika oz. skladno z delovnim procesom upravljavca infrastrukture, kar dogovorita izvajalec in naročnik. Za pravilno izvajanje procesa sprememb bo naročnik po podpisu pogodbe, oziroma pred prehodom v produkcijo zagotovil aktualno verzijo internega navodila »Upravljanje SPREMEB«.

Mesečno vzdrževanje zajema:

- Odprava napak in preventivno vzdrževanje, v katerega spadajo vse odprave napak in anomalij delovanja programske opreme na katerem koli od sistemov/okolij (produkcijsko, predprodukcijsko, testno) v skladu z dogovorom z naročnikom. V primeru zahteve naročnika to zajema tudi namestitev popravljenih različic v testno okolje, prenos produkcijske baze in po potrditvi s strani naročnika tudi prenos in namestitev popravka v produkcijsko okolje.
- Periodično (vsaj enkrat mesečno) preventivno preverjanje sistema. To zajema diagnostiko in odpravo morebitnih nekompatibilnosti programske opreme s sistemsko opremo. Nekompatibilnosti so lahko tudi posledica sprememb systemske opreme, na kateri bi po specifikacijah moral delovati programska oprema (na primer težave zaradi popravkov operacijskega sistema Windows). Izvajalec je o ugotovitvah dolžan pisno obvestiti naročnika.
- Analiza vseh zahtev naročnika za spremembo delovanja sistema in po potrebi nastavitve pred-produkcijskega ali testnega sistema za simulacijo ter spremljanje delovanja.
- Raznovrstna pojasnila glede delovanja sistemov, analize razlogov za zavračanje sprejetih dokumentov, ročni poseg v bazo mimo aplikacije na zahtevo naročnika.

- Sodelovanje z zaposlenimi v IT službi naročnika v primeru suma ali ugotovitve, da za neustrezno delovanje sistema obstaja vzročna povezava z nekim drugim IT sistemom naročnika.
- Druge aktivnosti, ki omogočajo nemoteno delovanje sistema v dogovorjenem obsegu (na primer težave pri izmenjavi podatkov z zunanjimi partnerji). Posodobitev in predložitev dokumentacije sistema ob nadgradnjah. To zajema opis funkcionalnosti, tehnična navodila, uporabniška navodila, opis opravljenih del (release notes), popis vplivov izvedenih sprememb na delovanje funkcionalnosti.

## 2.10 Licenciranje in izvorna koda

- IS ICMM mora vsebovati programsko opremo, ki licenčno ni sporna.
- Proizvajalec mora zagotavljati vsaj 5 letno življenjsko dobo programske opreme.
- Proizvajalec ne sme biti s strani države Slovenije ali EU opredeljen kot varnostno nesprejemljiv.
- Dobavitelj / implementator mora za čas življenjske dobe strojne/programske opreme zagotavljati varnostne popravke rešitve in zagotavljati delovanje ob nameščanju rednih varnostnih popravkov OS. (uporabljajo se določila SLA).
- Proizvajalec programske rešitve IS ICMM mora zagotoviti, da se skozi projekt razvoja in implementacije in v času vzdrževanja sistema zagotovi dostop do verzionirane izvorne kode produkta, ki je konča last naročnika.

## 2.11 Produkcijsko, , testno, razvojno okolje

Vse navedene zahteve v točkah 2.1 do 2.10 morajo biti upoštevane pri načrtovanju vseh treh okolij (Produkcijsko, Testno in Razvojno).

- Produkcijsko okolje IS ICMM je komunikacijsko in vsebinsko povezano v produkcijska okolja IS Eles, ki s deležniki v ICMM procesih.
- Testno okolje je komunikacijsko in vsebinsko povezano v testna okolja IS Eles, ki s deležniki v ICMM procesih. IS ICMM mora omogočati vse postopke za prenos produkcijskih podatkov v testno okolje (backup/restore produkcije na test,..), za katere morajo biti pripravljene in dokumentirane primerni postopki.
- Razvojno okolje IS ICMM je komunikacijsko in vsebinsko povezano v testna okolja IS Eles, ki s deležniki v ICMM procesih. Način uporabe podatkov se določi ob pripravi PZI.

## 2.12 Zakonske zahteve in interna pravila

- IEC 62351-100-8-2: Role-Based Access Control
- IEC 62325-504: Web Services
- ISO 27001: Information security, cybersecurity and privacy protection
- ISO 27031: IT disaster recovery
- PRI 5.3.1 TEMELJNA INFORMACIJSKO KIBERNETSKA VARNOSTNA POLITIKA DRUŽBE ELES D.O.O.
- OP K 7.5.4 P4 Navodilo »UPRAVLJANJE SPREMEMB«
- PRI K 7.5.4 P1\_1 Standardna uporabniška strojna oprema
- PRI K 7.5.4 P1\_2 Standardna uporabniška programska oprema,
- PRIK 7.5.4 P1\_3 Standardna strežniška programska oprema,
- PRIK 7.5.4.1 4 Sistemske nastavitve informacijskega sistema ELES.
- NA K 7.5.4.1 Varovanje in zaščita podatkov poslovno informacijskega sistema,
- NA K 7.5.4.2 Varnostno kopiranje podatkov v elektronski obliki,
- NA K 7.5.4.8 Metodologija razvoja programske opreme

## 2.13 Projekt za izvedbo (PZI) in Projekt izvedenih del (PID)

Dokument Projekta za Izvedbo (PZI) je namenjen natančnemu popisu in specifikacijam bodočega informacijskega sistema/aplikacije/modula. Na podlagi analize in specifikacij zahtev se v PZI določi seznam potrebnih gradnikov, poslovnih procesov, spletnih servisov in ostalih integracij. Na podlagi teh specifikacij se določi potrebne tehnološke standarde in tehnološke specifikacije za izvedbo ter arhitekturo sistema. Na ta način želi naročnik optimizirati arhitekturo in implementacijo sistema ter ob tem v največji smiselni meri vzpostaviti standardizacijo tehnoloških elementov ter s tem znižati skupne stroške lastništva centralne informacijske infrastrukture (v največji možni meri izogniti situaciji »vendor lock in«).

Dokument PZI mora vsebovati najmanj:

- funkcionalne specifikacije in funkcionalno dekompozicijo,
- seznam procesov z opisi,
- seznam gradnikov z opisi,
- specifikacije podatkovnih struktur,
- specifikacijo struktur XML,
- specifikacije spletnih storitev (API),
- specifikacijo aplikacije za prikaz podrobnosti delovanja vseh vključenih komponent,
- arhitekturo sistema za implementacijo (predlog uporabe vzorcev, topologija strežnikov, uporabljeni tehnološki standardi, tehnologija podatkovnih zbirk),
- načrt spletnih mest (žični okvir) s specifikacijami vsebin in funkcionalnostmi za uporabnike (npr. katere informacije vsebuje, kako naj zgleda uporabniški vmesnik,

kakšno uporabniško okolje bo ponujeno uporabniku, kako bodo organizirane vsebine, kakšne oblike iskanj bodo omogočene, do katere mere je mogoče doreči politiko umeščanja novih vsebin v portal, da se še zagotavlja preglednost),

- dokumentacijo v zvezi z ravnanjem s podatki (npr. definicijo sklopov podatkov), način obravnave podatkov skozi celoten življenjski cikel podatka (format hranjena, način izvajanja revizijske sledi, način ščitenja pred vpogledom, način umika na alternativen medij), način brisanja (ročno, batch obdelava, frekvenca),
- varnostne in zaščitne mehanizme,
- navedene in natančno popisane predvidene integracije z zunanjimi sistemi,
- terminski načrt.

Predvideno je, da izvajalec dokument PZI izdela po izvedeni analizi zahtev.

Dokument PZI potrdi naročnik.

Po zaključku del, mora izvajalec izdelati projekt izvedenih del (PID), skupaj z upravljavskimi, vzdrževalnimi in uporabniškimi navodili. Po izvedenem šolanju za upravljanje, administracijo in uporabo, naročnik potrdi PID in predana navodila.