REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO
DIREKTORAT ZA INFORMATIKO

Tržaška cesta 21, 1000 Ljubljana

T: 01 478 86 51
F: 01 478 86 49
E: gp.mju@gov.si
www.mju.gov.si

Generične Tehnološke Zahteve

(GTZ)

Za razvoj informacijskih rešitev

V2.2.9

Kazalo vsebine

1

O tem dokumentu:

Dokument je sestavljen iz serije zahtev[1], ki jih zastavlja tehnološko okolje, kamor se uvrščajo sistemi.
Zahteve so urejene v vsebinsko sorodne skupine, ki so obravnavane v posameznih poglavjih.
Posamezna zahteva je označena z govorečo šifro v formatu:
GTZ-AAA…-BBB…-YY
kjer je:
GTZ – oznaka, ki pove, da gre za generalno tehnološko zahtevo
AAA – govoreča oznaka skupine zahtev
BBB – govoreča oznaka zahteve
YY – zaporedna številka točke zahteve BBB

V primeru, da se zahteva pod posamezno oznako razlikuje glede na ciljno tehnološko okolje, se to pod posamezno oznako eksplicitno navede.

Način ravnanja z dokumentom	Dokument se s svojimi prilogami kot nedeljiv element pripenja kot priloga razpisnim dokumentacijam za sisteme, ki so oz. bodo umeščeni na infrastrukturo MJU. Zahteve upravljavca infrastrukture predstavljajo obvezni del specifikacij predmetnega naročila.
Način upravljanja s spremembami	Z dokumentom upravlja MJU kot upravljavec infrastrukturnega okolja. MJU/DI tudi izvaja spremembe nad dokumentom; tako se npr dokument po potrebi prilagodi na specifike razpisne dokumentacije za vsak razpis posebej.

Spremembe dokumenta	
28.2.2012	Verzija 1.0.1
4.6.2012	Verzija 1.0.2: Uvedba označevanja posameznih zahtev, dodano poglavje o ravnanju z dokumentom
6.6.2012	Dodani odstavki: bazni računi, pojasnilo k semaforčkom, optimizacija zbirk, nivoji logiranja;
6.7.2012	Popravki GTZ-PROJEKT-PZI-07/ GTZ-PROJEKT-PZI-70, tipkarske napake, natančnejša opredelitev nadzornih mehanizmov, razdelitev točke GTZ-NADZOR-SYS-30 v dve: GTZ-NADZOR-SYS-30 za avtomatsko sistemsko preverjanje in GTZ-NADZOR-SYS-35 za »ročno nadzorno konzolo«
9.10.2012	Zbrisanih nekaj nerelevantnih stavkov v glavi dokumenta
27.11.2012	Dodan: GTZ-STANDARDI-SPL-20 Zahteve za Ipv6 podporo v programski opremi.
13.12.2012	Podrobnejše opredelitve dostopov do podatkovne zbirke s strani modulov.
17.12.2012	Dodana opredelitve v zvezi z informacijsko varnostjo
5.5.2013	Dodane opredelitve glede portalne infrastrukture, admin modulov
5.7.2013	Dodane opredelitve glede obvladovanja nadzora na uporabo osebnih podatkov
22.2013	Sprememba iz MNZJU na MNZ/DIES
7.8.2014	Popravek povezave na varnostno politiko

[1] V dokumentu se pojavljajo tudi deli besedila, ki niso neposredne zahteve za sistem same po sebi, vendar pojasnjujejo okvir oz gabarite, v okviru katere se sistem umešča. Da sistem ni v nasprotju s temi okviri, je zahteva. Primer: »Tehnološko okolje Informacijskega sistema (v nadaljevanju: Sistem) bo v celoti nameščeno na obstoječo infrastrukturo v upravljanju Ministrstva za javno upravo, Direktorata za informatiko (MJU/DI). Predvidena je namestitev na primarni lokaciji ter lokaciji nadomestnega centra (kolokacija).«

10.10.2014	Verzija v.1.11.2: popravljena dikcija v zvezi s specifikacijami, ki so del PZI (točka GTZ-PROJEKT-PZI-50), popravljena referenca na priporočila Informacijskega pooblaščenca (GTZ-NADZOR-REVIZIJA-30), popravljena glava dokumenta in reference na naziv organa, ki upravlja z dokumentom.
18.05.2016	Verzija v11.2-1: Uskladitev oznak z Zakonom o državni upravi, odprava slovničnih napak
16.9.2016	Uskladitev nabora ciljnih možnih tehnoloških izvajalnih okolij, dodatek poglavij GTZ-POSTAVITEV-CONFIG-10 in GTZ-POSTAVITEV-PROXY-10
6.10.2016	Večja dodelava v smislu: - organizacije posameznih zahtev, nekatere zahteve so bile preštevilčene, nekatera besedila jasneje spisana, - dodane zahteve za sisteme, ki jih upravitelj lahko umesti na oblačno .Net infrastrukturo, - kjer so zahteve za razpoložljivi tehnološki platformi Java EE in .Net razlikujejo zaradi tehnoloških ali licenčnih specifik, se posamezna zahteva definira za vsako tehnološko platformo posebej, - sprememba na področju zaželjene časovnice: zaradi uvedbe varnostnega testiranja z orodjem CheckMarx, ki ga je v razvojni cikel smiselno uvesti v čimzgodnejši fazi, zahteva GTZ-OKOLJE-NIVOJI-20 spodbuja k oddaji kode v ustrezen repozitorij v čimzgodnejši fazi razvoja; dodana tudi GTZ-VARNOST-TESTI-10 - v zahtevi GTZ-ODJEMALCI-NEODV-10 se več pozornosti nameni načrtovanju podpori odjemalcem, ki so za ciljni nabor uporabnikov primerni (skupina referentov za šalterji ima drugačno naravo in drugačne zahteve kot skupa državljanov) - GTZ-PROJEKT-PZI-11 sodelovanje upravljavca infrastrukture v fazi PZI je obvezno - GTZ-PROJEKT-METODOLOGIJA-30 pokritost z unit testi - GTZ-OPTIMIZACIJA-SPL-40 nivo sql poizvedb mora biti obvladovan - GTZ-POSTAVITVE-TUP-30 build proces
30.12.2016	Sprememba dikcije brez spremembe koncepta predvsem v poglavjih GTZ-STANDARDI-DEV-10, GTZ-POSTAVITVE-TUP-30
7.2.2017	Jasnejša dikcija brez bistvene spremembe koncepta v poglavjih: - »O tem dokumentu« - jasneje definirana vloga dokumenta GTZ ter vloge zahtev upravljavca infrastrukture, - skozi celoten dokument jasnejša razmejitev vlog naročnika in upravitelja infrastrukture (GTZ-OKOLJE-SPL-10, GTZ-OKOLJE-NIVOJI-30, GTZ-OPTIMIZACIJA-SPL-30, GTZ-PROJEKT-METODOLOGIJA-10, GTZ-PROJEKT-METODOLOGIJA-20, GTZ-VARNOST-TESTI-10 , GTZ-VARNOST-TESTI-20…), - GTZ-OKOLJE-SPL-20: jasnejša zahteva po možnosti teka več vzporednih kopij - GTZ-OKOLJE-NIVOJI-10: jasnejša razlaga namena Apache strežnika, - GTZ-OKOLJE-NIVOJI-40: jasnejša definicija, - natančneje definirana želja v zvezi s pričakovanji po 'lahkih' odjemalcih (GTZ-ARHITEKTURA-NIVOJI-10, GTZ-ODJEMALCI-NEODV-10), - GTZ-PROJEKT-PZI-50: jasnejša definicija, - GTZ-PROJEKT-DOKUMENTACIJA-10: odvzem točke 9 v zvezi z zahtevo, da izvajalno podjetje pripravi konkretno namestitveno shemo ter konkretnimi podatki o strojni opremi, - GTZ-POSTAVITVE-TUP-10: naslovljeno vprašanje postavljanja dodatnih okolij (poleg testnega, uvajalnega, produkcijskega), - GTZ-NADZOR-SYS-35: aplikacije brez integracij izvzete iz zahteve;
2.3.2017	Omiljena zahteva GTZ-OKOLJE-NIVOJI-40, Popravljen napačen sklic v okviru zahteve GTZ-PROJEKT-PZI-30,

		Jasnejša dikcija v zvezi z razmejitvijo vlog naročnika in upravitelja infrastrukture v točkah GTZ-ARHITEKTURA-NIVOJI-10,GTZ-PROJEKT-METODOLOGIJA-10;
24.05.2017	2.2.4	Prilagoditev dikcije v zahtevi GTZ-VARNOST-NORMATIVI-20
1.9.2017	2.2.5	Prilagoditev dikcije v zahtevi GTZ-VARNOST-NORMATIVI-10 pregled -> pregledi
1.9.2017	2.2.5	Dodana zahteva: GTZ-VARNOST-OSEBNI-PODATKI-10
4.9.2017	2.2.5	Poglavje: GTZ-NADZOR-SYS-35 razširjeno z okolji in moduli sistema. Izvedene oblikovne izboljšave.
4.10.2017	2.2.6	Dodatek zahteve »Statistične obdelave ne smejo negativno vplivati na delovanje transakcijskega dela sistema.« v GTZ-NADZOR-STAT-10
5.03.2018	2.2.7	Zahteva GTZ-NADZOR-SYS-40, ki opisuje implementacijo podrobnejše statistike rabe sistema, se briše. Odločitev o izdelavi podrobnejše statistike je torej predmet odločitve posamičnega projekta, Zahteva GTZ-NADZOR-PROCESI-10 dobi pojasnilni stavek;
7.3.2018	2.2.7	Popravek podnaslova iz »sistemov« na »rešitev«
26.04.2018	2.2.8	Sprememba v točki GTZ-VARNOST-PRAKSE-10, ker je dokument »Politika informacijske varnosti« zamenjala »Uredba o informacijski varnosti v državni upravi«;
11.2.2021	2.2.9	Dodana pravila za pripravo aplikacij na Docker okolju MJU: - Posodobitev, preštevilčenje poglavij in kazala, - dopolnjeno besedilo pravil: GTZ-OKOLJE-NEODV-10, - posodobljen URL v *GTZ-STANDARDI-SPL-20,* - *sprememba GTZ-PROJEKT-PZI-11, namesto MJU potrdi, MJU uskladi,* - novo poglavje "1.5 Zahteve v zvezi s kontejneriziranimi aplikacijami" z zahtevami GTZ-VSEBNIKI-*, - dopolnjeno poglavje "1.6 Splošna postavitvena pravila" z referenco na GTZ-VSEBNIKI-ENV* pravila, - Popravek v točki GTZ-OKOLJE-NIVOJI-30: Izraz Jboss zamenjan za Wildfly (odprtokodni), - posodobitev *GTZ-PROJEKT-SPREMEMBE-40, posodobljen URL, posodobljena tabela strukture SVN;*.

1.0 Tehnološko okolje

GTZ-OKOJE-SPL-10 Tehnološko okolje Informacijskega sistema (v nadaljevanju: Sistem) bo v celoti nameščeno na obstoječo infrastrukturo v upravljanju Ministrstva za javno upravo, Direktorata za informatiko (MJU/DI). Poleg namestitve na primarni lokaciji se upravitelj infrastrukture lahko odloči tudi za namestitev celotnega sistema ali njegovega dela na lokaciji nadomestnega centra (kolokacija).

GTZ-OKOLJE-SPL-20 Glavne značilnosti infrastrukture:
- na nivoju tehnološke infrastrukture:
  a. infrastruktura naj bi bila postavljena v luči zagotavljanja visoke razpoložljivosti, skalabilnosti ter prenosljivosti na različno strojno opremo,
  b. naročnik lahko sistem ali dele sistema (modula) namesti bodisi na fizične bodisi na virtualizirane strežnike,
  c. uporabljena je lahko strojna stikalna oprema za porazdelitev bremen ali pa strežnik baziran na Apache spletni strežbi, za večje obremenitve so predvideni ločeni sklopi po več instanc spletnih/aplikacijskih strežnikov v delu strežbe spletnih storitev,
- na nivoju umestitve modulov na infrastrukturo:
  d. samo ogrodje ter spremljajoči centralni moduli se postavljajo ločeno za potrebe storitev (bodisi za človeške, torej GUI, bodisi za aplikacijske uporabnike, torej spletne storitve),
  e. predvideti je potrebno, da se dodatna aktivna kopija aplikacijskih komponent lahko postavi na sekundarni lokaciji (na aplikacijskem nivoju mora biti možno vzpostaviti več hkratno aktivno delujočih vzporednih instanc aplikacijskih komponent),
  f. moduli ali komponente, ki vsebujejo funkcionalnosti administracije informacijskega sistema se nameščajo izključno in samo na aplikacijske strežnike, ki so dostopni samo znotraj omrežja državnih organov (intranet);

GTZ-OKOLJE-NEODV-10
Infrastrukturne tehnološke zahteve za informacijskega sistema morajo biti neodvisne od blagovne znamke dobaviteljev strojne opreme, ali od platforme za virtualizacijo sistemov ali v primeru Docker tehnologij od okolja za orkestracijo.
S tem pričakovanjem upravitelj infrastrukture želi zagotoviti, da bo rešitev delovala na naročnikovi obstoječi infrastrukturi.
Naročnik si pridržuje pravico do spremembe obstoječe tehnologije infrastrukture.

GTZ-OKOLJE-NEODV-20: Sistem/aplikacija/moduli ne smejo biti zaklenjena na število procesorjev, količino spomina, velikost diska ali na kakršnekoli druge programske in strojne parametre.

GTZ-OKOLJE-NIVOJI-01 Sistem je tro ali večnivojske arhitekture z lahkim odjemalcem (spletnim brskalnikom).

GTZ-OKOLJE-NIVOJI-10 Za strego večjih obsegov statičnih datotek (html, slike, …) je predviden odprtokodni strežnik Apache.

GTZ-OKOLJE-NIVOJI-20 Za aplikacijski nivo Sistema je predvideno ciljno izvajalno okolje po specifikacijah programskega jezika.
Na razpolago sta izvajalno okolje po specifikacijah Java EE in izvajalno okolje za.NET verzije 3.5 ali višje.
Uspešna namestitev in uspešna izvedba funkcionalnih testov na testnem izvajalnem okolju je prva kontrolna točka v procesu implementacije Sistema na ciljno infrastrukturo.

Prva namestitev na testno izvajalno okolje pa se izvede takoj, ko je struktura (skelet) aplikacije sestavljen do te mere, da uporablja vse tehnološke rešitve, zato da se preveri skladnost z obstoječo infrastrukturo ter se lahko začnejo izvajati varnostna testiranja kode (Checkmarx).

GTZ-OKOLJE-NIVOJI-30

Upravitelj infrastrukture licenčno krije osnovno izvajalno okolje.

Predvidene implementacije osnovnega izvajalnega okolja na ciljni infrastrukturi so:

- za izvajalno okolje Java EE: javanske aplikacije se najprej namestijo na okolje Wildfly kot referenčno izvajalno okolje za Java EE. S tem se zagotovi skladnost aplikacije z Java EE standardi
  Upravljavec infrastrukture se po uspešnem testu na testnem okolju lahko odloči, da se bo sistem namestil tudi na drugo na upravljavčevi infrastrukturi obstoječe okolje (izvajalno okolje, ki izhaja iz licenčnega ali odprtokodnega poslovnega modela). Zato je potrebno, da je tehnološka zasnova aplikacijskega dela zasnovana tako, da je čim bolj neodvisna od posameznih implementacij izvajalnih okolij znotraj rešitev istega programskega jezika,

- za izvajalno okolje .Net: predviden je spletni/aplikacijski strežnik IIS,

Upravitelj infrastrukture ne krije nobenih stroškov morebitnih dodatnih plačljivih tehnologij, storitev, ogrodij, aplikacij in drugih plačljivih dodatkov. Stroške za uporabo morebitnih plačljivih tehnologij, storitev, ogrodij, aplikacij in drugih plačljivih dodatkov nosi projekt in ne upravitelj infrastrukture, kar velja za ves čas življenjske dobe sistema.

GTZ-OKOLJE-NIVOJI-40 Za podatkovni nivo je predvidena relacijska podatkovna zbirka, ki podpira standard SQL.

1.1 Tehnološki standardi in specifikacije

GTZ-STANDARDI-SPL-10 V največji možni meri, ki jo še dopušča ciljno izvajalno okolje, naj bodo uporabljeni sodobni, odprti in neodvisni tehnološki standardi[2] in specifikacije pri razvoju spletnih rešitev.

GTZ-STANDARDI-SPL-20 Zahteve za IPv6 podporo v programski opremi.
Vsa programska oprema, ki sestavlja informacijski sistem, mora podpirati IPv4 in IPv6 v vseh kombinacijah komunikacije (samo IPv4, samo IPv6 in IPv4 ter IPv6 hkrati – dual stack). Če programska oprema vključuje omrežne parametre v svojih lokalnih ali oddaljenih nastavitvah, mora enakovredno podpirati tudi konfiguracijo IPv6 parametrov.
Možnosti, za obdelavo omrežnih naslovov, ki jih ima programska oprema za protokol IPv4, morajo biti na voljo tudi za protokol IPv6. Lastnosti informacijskega sistema se ne bi smele manifestirati v različni obravnavi, ko programska oprema komunicira po IPv4 ali po IPv6.
(Vir: https://www.ripe.net/publications/docs/ripe-554#requirements_ipv6_support)

GTZ-STANDARDI-DEV-10

(1) Definicija odprtega standarda:

- Odprti standard je dobro dokumentiran in je celotna specifikacija javno dostopna
- Odprti standard lahko prosto implementiramo brez ekonomskih, političnih ali pravnih omejitev glede implementacije in uporabe.
- Odprti standard je standardiziran in ga vzdržuje odprta neprofitna organizacija v odprtem procesu

2

Koda, ki je rezultat predmetnega javnega naročila, mora biti predana na način, da se dostavljeni izdelki lahko v celoti vključijo v procedure avtomatskega prevajanja v izvršljivo obliko in grajenja namestitvenih paketov z vsemi odvisnostmi na okolju, vzpostavljenem na infrastrukturi MJU.

Ponudnik rešitve predmetnega razpisa mora sposobnost naročnika, da samostojno izgradi končno delujočo s ciljno infrastrukturo združljivo aplikacijo vključno z namestitveno proceduro, zagotoviti brez dodatnih licenčnih stroškov za naročnika ali upravitelja infrastrukture.

1.2 Tehnološka neodvisnost na strani odjemalcev

GTZ-ODJEMALCI-NEODV-10 Informacijska rešitev, ki je predmet javnega naročila, mora omogočati uporabnikom nemoteno delo z uporabo vseh relevantnih tehnologij (npr MS IE, Mozilla Firefox, Chrome) odjemalca in operacijskih sistemov (npr MS WIN 7, Linux, Mac OS) brez namestitvenih ali konfiguracijskih posegov na strani odjemalca, vključujoč brskalnik, operacijski sistem ali katerokoli komponento uporabniške delovne postaje.

Točnejši nabor relevantnih tehnologij spletnih odjemalcev se določi bodisi na nivoju / v času same razpisne dokumentacije bodisi najkasneje v PZI in to glede na ciljno skupino uporabnikov.[3]

1.3 Dokument PZI

GTZ-PROJEKT-PZI-10 Dokument Projekta za Izvedbo (PZI) je namenjen natančnemu popisu in specifikacijam bodočega informacijskega sistema/aplikacije/modula. MJU/DI želi, da se na podlagi funkcionalne dekompozicije določi seznam potrebnih gradnikov, poslovnih procesov, spletnih servisov in integracij.
Predvideno je, da se dokument PZI izdela po fazi analize vendar pred zaključkom faze načrtovanja (v prvi tretjini faze načrtovanja).

GTZ-PROJEKT-PZI-11 Dokument PZI potrdi naročnik na podlagi soglasja lastnika in upravljavca centralne infrastrukture MJU/DI, v primeru, da naročnik ni MJU/DI.
MJU/DI kot upravljavec centralne informacijske infrastrukture dokumentacijo PZI uskladi s stališča uporabe/izmenjave dobrih praks, uporabe centralnih gradnikov in identifikacije optimalne ter zanesljive postavitve.
Na ta način želi MJU/DI optimizirati arhitekturo in implementacijo sistema na obstoječo infrastrukturo 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«).

GTZ-PROJEKT-PZI-20 Na podlagi teh specifikacij se šele določi potrebne tehnološke standarde in tehnološke specifikacije za izvedbo ter arhitektura sistema.

GTZ-PROJEKT-PZI-30 V primeru, da izvajalec predlaga tehnološki standard ali specifikacije, ki ne ustrezajo definiciji odprtosti in neodvisnosti (v okviru ***GTZ-STANDARDI-SPL-10***) mora to odločitev posebej obrazložiti.

GTZ-PROJEKT-PZI-31 Nabor in topologijo aplikacijskih strežnikov in nabor podatkovnih zbirk (podatkovni nivo), ki jih mora aplikacija podpirati, se določi v dokumentu PZI (v primeru novega sistema oziroma večjih dograditev le-tega) ali drugi ustrezni projektni dokumentaciji (v primeru obstoječega sistema).

GTZ-PROJEKT-PZI-50 Dokument PZI vsebuje najmanj:

[3] Primer: nabor relevantnih tehnologij bo torej lahko drugačen, če je razpisana rešitev namenjena uporabniški skupini referentov na upravnih enotah s standardiziranim delovnim okoljem, ali pa če je razpisana rešitev za najširši nabor internetnih uporabnikov – državljanov.

1) Specifikacija poslovnih procesov, ki jih bo rešitev podprla, s komentiranimi diagrami po UML standardu (obvezno vključujoč vsaj primere uporabe, sekvenčne diagrame ter druge diagrame glede na obravnavano tematiko),
2) funkcionalna dekompozicija
3) seznam poslovnih procesov z opisi,
4) seznam gradnikov z opisi,
5) popis uporabljenih tehnologij in/ali morebitne dodatne opreme,
6) specifikacije podatkovnih struktur
7) specifikacija XML struktur
8) specifikacije spletnih storitev
9) specifikacija aplikacije za prikaz podrobnosti delovanja vseh vključenih komponent, kadar se taka aplikacija implementira,
10) arhitekturo sistema za implementacijo z določenimi/navedenimi povezavami med komponentami (predlog uporabe vzorcev, topologija strežnikov, uporabljeni tehnološki standardi, protokoli, tehnologija podatkovnih zbirk),
11) varnostne in zaščitne mehanizme,
12) navedene in popisane predvidene integracije z zunanjimi sistemi,
13) terminski načrt
14) poglavje z obravnavo zahtev dokumenta GTZ v verziji, ki je bila priložena predmetnem naročilu, kjer je za vsako zahtevo razvidno ali je implementacija zajeta v celoti ali pa so predvidena odstopanja s pripadajočo obrazložitvijo;

1.4 Splošne arhitekturne smernice

GTZ-ARHITEKTURA-NIVOJI-10 Arhitektura sistema mora biti spletna, več-nivojska (podatkovna zbirka, aplikacijski strežniki, spletni strežniki, spletni brskalnik), nekateri deli aplikacij so zaprti za "zunanje" uporabnike (dostop le iz privatnega državnega omrežja HKOM).
Za uporabniško (odjemalsko) stran je predvidena uporaba spletnega brskalnika, ki sodi med širše uporabljane (npr Internet Explorer ali nasledniki, Firefox, Chrome, …). Informacijska reštev, ki je predmet tega naročila mora delovati brez uporabe posebnih odjemalcev ali vtičnikov, razen ko tako eksplicitno določa naročnik v razpisni dokumenciji.

GTZ-ARHITEKTURA-MODULARNOST-10 Sistem mora biti zgrajen modularno. Predstavitveni nivo mora biti logično ločen od poslovne logike. Arhitektura mora upoštevati varnostna pravila in dobre prakse s področja informacijske varnosti.
Administrativne funkcije morajo biti ločene od ostalih v samostojen (samostojno namestljiv/naslovljiv) modul.

GTZ-PROJEKT-PZI-10 Arhitektura se zasnuje skupaj z upravljavcem infrastrukture (MJU/DI) in se potrdi v okviru PZI.

1.5 Zahteve v zvezi s tehnologijo vsebnikov

Poglavje je relevantno v primerih uporabe tehnologije vsebnikov (docker). Za aplikacije v vsebniških (Docker) tehnologijah veljajo tudi vse ostale zahteve v GTZ.

GTZ-VSEBNIKI-IMG-10:
Izvorne (začetne, FROM) docker slike morajo biti na voljo v javnih docker registrih (npr dockerhub) ter so predmet usklajevanja tekom pregleda PZI dokumentacije.
Izvorne slike vsebnikov morajo biti v skladu z vsemi ostalimi pravili GTZ ali GTZ-LOP ter so prav tako kot izvorna koda predmet varnostnega preverjanja.

GTZ-VSEBNIKI-IMG-20: V okolju upravitelja infrastrukture je uporabljen lasten repozitorij za hrambo slik vsebnikov. Docker vsebniki se startajo izključno iz tega repozitorija.

GTZ-VSEBNIKI-IMG-30: Končne docker slike se gradijo v okolju upravitelja infrastrukture. Datoteka dockerfile se smatra za del izvorne kode.

GTZ-VSEBNIKI-LOG-10: Za potrebe zbiranja in vpogleda v dnevnike vsebniških aplikacij je na centralni infrastrukturi postavljen sklad ElasticSearch-Kibana, kjer je naročnikom in razvojnim ekipam omogočen dostop do aplikacijskih dnevnikov (log)

GTZ-VSEBNIKI-LOG-20: Oblika in način zapisovanja v dnevnike morata biti prilagodljiva; običajno se nastavi format za ELK in logiranje na stdout.

GTZ-VSEBNIKI-ARH-10: Moduli morajo biti "stateless", razen izjemoma, kjer drugačna rešitev ni možna

GTZ-VSEBNIKI-ENV-10: Trenutno se za orkestracijo uporablja tehnologija vsebnikov Docker SWARM. Aplikacija ne sme biti odvisna od izbire orkestratorja, lahko pa se zaveda SWARM routing - mesh mrežnih povezav. Posamezni servisi so znotraj aplikacije mrežno naslovljivi z imenom servisa

GTZ-VSEBNIKI-ENV-20: Možnost trajne hrambe (persistent storage) za kontejnerje je zagotovljena na naslednje načine:
1) skrivnosti (gesla, certifikati, …) : preko možnost "docker secrets",
2) konfiguracije (razne konfiguracijske datoteke) : preko možnosti "docker configs" ali po potrebi preko načina 3,
3) podatki : preko možnosti "docker volume" ali "bind mount" na distribuirane file sisteme.

GTZ-VSEBNIKI-ENV-30: V gručah vsebnikov (Docker SWARM cluster) sobiva več informacijskih rešitev. Poimenovanje posameznih mikrostoritev (vsebniških servisov) se določi skupaj s sistemskimi ekipami upravitelja infrastrukture, pri čemer imajo imena mikrostoritev (servisov) za predpono ime informacijske rešitve (aplikacije).

GTZ-VSEBNIKI-ENV-40:
Nameščanje sistemskih Docker komponent na virtualne strežnike, vzpostavitev Docker gruče in konfiguracija orkestratorja NI stvar aplikacije.
Razvijalec naj predpostavi obstoječe v naprej pripravljeno izvajalno okolje, ki ga vzpostavi upravitelj infrastrukture

1.6 Splošna postavitvena pravila[4]

GTZ-POSTAVITEV-CONE-10 Moduli, do katerih dostopajo uporabniki, ki nimajo dostopa do komunikacijskega omrežja državnih organov (v nadaljevanju HKOM), se nameščajo v DMZ območje (segment požarne pregrade in segmentih stikala za porazdelitev bremen – »Content Switch«) oziroma drugo področje, eksplicitno namenjeno dostopu iz internetnega področja.

GTZ-POSTAVITEV-CONE-20 Moduli, do katerih dostopajo izključno HKOM uporabniki, se nameščajo znotraj intraneta komunikacijskega omrežja državnih organov. Točna postavitev modulov pa se določa, ko so znani gabariti posameznega modula (značilnost aplikacije, nabor uporabnikov, nivo zahtevane varnosti, pričakovane obremenitve ipd.) skupaj s strokovnjaki Ministrstva za javno upravo.

GTZ-POSTAVITEV-CONFIG-10 nastavitve (kot so proxy, URL, lokacija truststora, certifikatov …) morajo biti v zunanji konfiguracijski datoteki, ki se ne prepisuje z deployem spletnega servisa/modula in je specifična strežniku, na katerem modul teče.

[4] V primeru docker aplikacij glej tudi GTZ-VSEBNIKI-ENV-*

GTZ-POSTAVITEV-PROXY-10 v primerih, ko sistem dostopa do internetnih spletišč ali spletišč nekaterih pridruženih omrežjih, je za http(s) komunikacijo predpisana uporaba internega posrednika (proxy strežnik) z namenom enoznačne predstavite IP naslova. S tem se omogoča enostavna selitev/dodajanje aplikacije na drug strežnik.
Sistem mora omogočati dostop do ciljanih spletišč tako neposredno, kot posredno, kar se določa v konfiguracijski datoteki (GTZ-POSTAVITEV-CONFIG-10)

1.7 Način dostopa do podatkovne zbirke

GTZ-BAZA-DOSTOP-10 Zahteva upravitelja infrastrukture je, da se aplikacija/modul na bazo prijavlja z računom (account/uporabnik) s tistim minimalnim naborom pravic, ki aplikaciji še omogoča delovanje oziroma izvrševanje poslovnih funkcij, ki jih aplikacija implementira.
V nadaljevanju je zahteva pod to oznako spisana v terminologiji sveta Oracle podatkovnih zbirk. V primeru implementacije sistema na Microsoft SQL zbirko je zahtevo potrebno povzeti smiselno ekvivalentno.

Aplikacija naj se v nobenem primeru na bazo ne prijavlja s povezavo (bazno sejo), vzpostavljeno neposredno na shemo, ki je lastnik baznih objektov (tabel, baznih procedur etc). Aplikacija do baze dostopa s prijavo na posebnega, za dano aplikacijo/modul namensko postavljenega baznega uporabnika (create user …), ki ima dodeljene le pravice (grant execute) do izvajanja tistih namensko spisanih baznih procedur/funkcij, ki jih za svoje delovanje nujno potrebuje.
Bazni uporabnik, namenjen prijavi na bazo, se ustvari za vsak samostojen modul aplikacije/sistema posebej (npr: modul portal, modul spletne storitve, modul za administracijo…)[5]

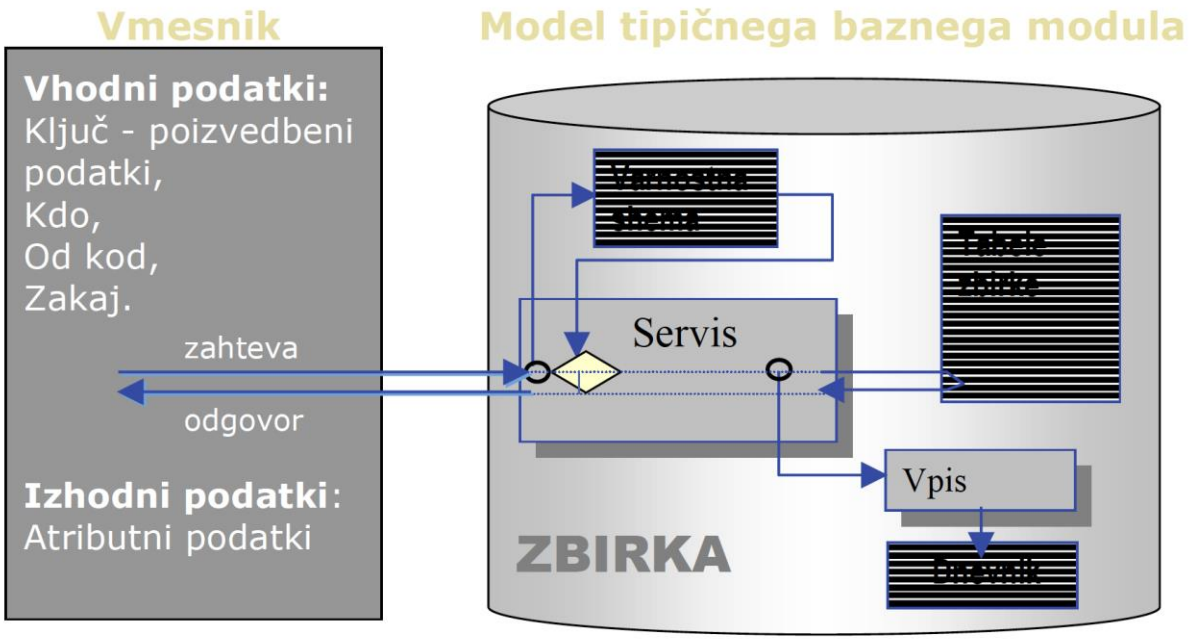
GTZ-BAZA-DOSTOP-20
Spletni moduli, dostopni iz internetnega območja ali extraneta (povezav tujih sistemov) oziroma spletni servisi, ki so potrebni za integracije s tujimi sistemi, naj do baze **ne** dostopajo neposredno preko SQL poizvedb nad tabelami, ampak:

- bodisi preko klicev baznih procedur, ki jih potrebujejo za svojo poslovno logiko (pri čemer naj ima account, s katerim se modul veže na bazo, ima pravico samo do izvajanja teh baznih procedur),
- bodisi preko klicev namenskega nivoja spletnih storitev v ta namen (glej tudi GTZ_BAZA_DOSTOP-10).

Glede na specifično situacijo, lahko ta bazna procedura opravlja tudi kake druge potrebne funkcije, na primer ustvarjanje revizijskih sledi, preverjanje pravic izvajanja v varnostni shemi etc.

[5] Primer: sistem 'foobar' z enim administrativnim in enim vpogledovalnim modulom za javnost bi torej potreboval (vsaj) tele sheme:

- foobar_own – lastnik tabel,
- foobar_admin_app – (glede na funkcionalnosti admin aplikacije verjetno) samo select, execute (hipotetično insert, v kolikor je z naročnikom tako dogovorjeno),
- foobar_web_app – samo execute za bazni servis za vpogled



Slika 1. Okvirni princip modela baznega modula.

GTZ-BAZA-DOSTOP-30 Izjema za pravilo *GTZ-BAZA-DOSTOP-20* je bralni način dostopa do šifrantov in klasifikacij ter list vrednosti, ki se kateri se lahko izvede preko »podatkovnih pogledov« (database views). Prav tako se dopušča izjema za sklop za urejanje portalnih vsebin (CMS), ki se nanašajo izključno na krmiljenje CMS funkcij. Navedene izjeme naročnik potrdi na nivoju dokumenta PZI (projekt za izvedbo) ali pa na nivoju dokumenta VDP

GTZ-BAZA-DOSTOP-40 Način izvedbe preostalega dela aplikacijskega nivoja se dogovori z upravljavcem infrastrukture v okviru PZI, pri čemer se tehta med vložkom v razvoj, predvidenimi stroški vzdrževanja (razvojni vidik, sistemski vidik), morebitnimi specifičnimi lastnostni sistema ali posameznih transakcij v okviru tega sistema, izkušnjami sistemskih in razvojnih ekip ter drugimi dejavniki, ki so znani v času sestavljanja PZI.

1.8 Metodologija razvoja ter upravljanje s spremembami programske opreme

GTZ-PROJEKT-METODOLOGIJA-10 Upravljavec infrastrukture izrecno ne predpisuje konkretne metodologije razvoja (lahko pa jo predpiše naročnik) programske opreme, vendar mora izvajalec navesti, katero metodologijo uporablja in kateri izdelki, poleg tistih, ki so eksplicitno že navedeni v okviru danega razpisa, bodo rezultat razvoja.

GTZ-PROJEKT-METODOLOGIJA-20 Upravljavec infrastrukture pričakuje, da ima izvajalec vzpostavljen proces v okviru razvojne metodologije, ki izdelke razvoja hrani v repozitoriju izvorne kode (SVN (Sub)VersionControl, GIT ali primerljivo) ter da sproti izvaja teste (Unit testi).

GTZ-PROJEKT-METODOLOGIJA-30 Koda, odložena v naročnikovo SVN okolje, naj bo primerno pokrita z unit testi. Stopnja pokritosti kode se določi na nivoju PZI.

GTZ-PROJEKT-SPREMEMBE-10 Od izvajalca se pričakuje, da ima izdelane in uveljavljene postopke obvladovanja sprememb (repozitorij, številčenje različic). Izvajalec je dolžan voditi evidenco, vse spremembe ustrezno označevati ter dokumentirati. Verzija naj bo jasno razvidna iz uporabniškega vmesnika modula (npr: 'vizitka', 'noga', itd).
Pravilo velja tako za spremembe aplikacije, za spremembe baznih objektov ter za spremembe spremljajoče dokumentacije.

GTZ-PROJEKT-SPREMEMBE-20 Za vse spremembe, ki jih izvajalec načrtuje, mora izvesti postopke obveščanja tako naročnika kot upravljavca infrastrukture.

GTZ-PROJEKT-SPREMEMBE-25 Če nov sistem/aplikacija/modul zahteva dodatne nastavitve (nastavitve, ki odstopajo iz okvira danega ciljnega okolja), programsko opremo ali druge pogoje, mora izvajalec na to naročnika in upravljalca infrastrukture predhodno opozoriti že fazi PZI. Naročnik lahko te pogoje sprejme, ali pa jih zavrne in zahteva spremembe v sami aplikaciji,

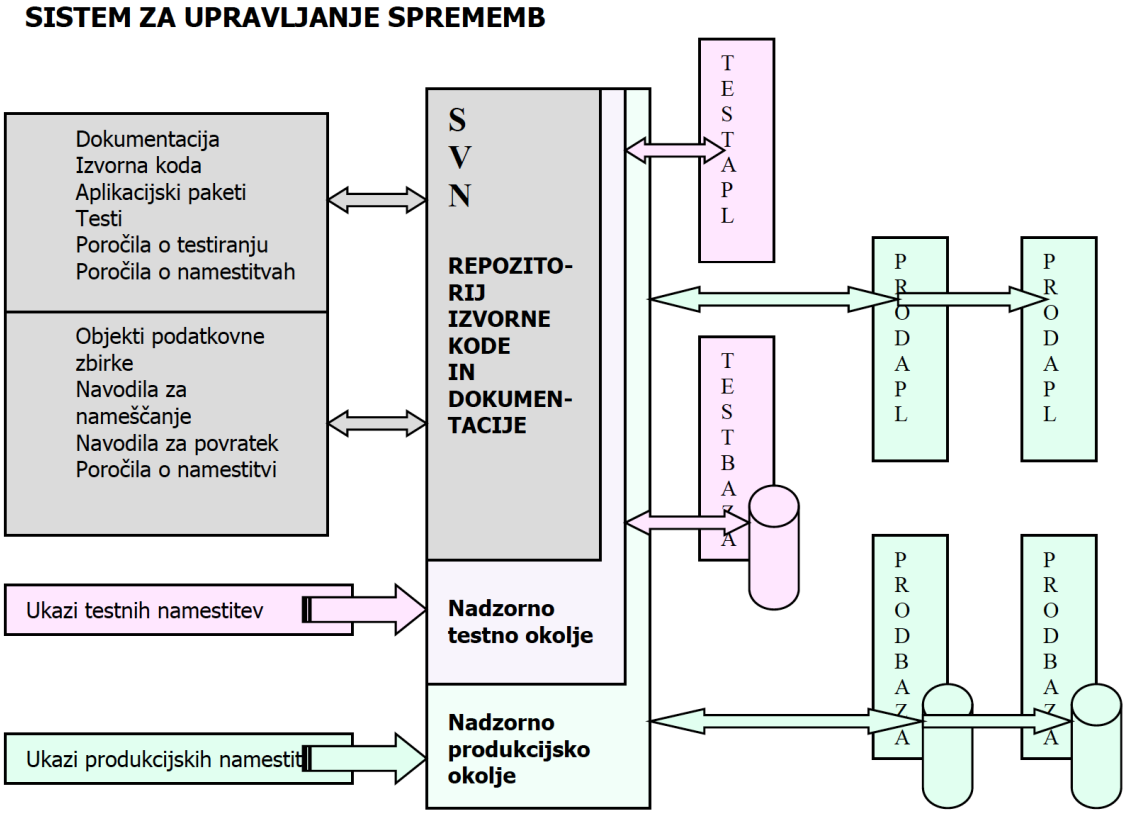
GTZ-PROJEKT-SPREMEMBE-30 Izdelki razvoja se posredujejo/odlagajo naročniku v namenski »SVN repozitorij« - strežnik za hranjenje verzij oziroma sistem za upravljanje sprememb. Repozitorij izvorne kode ima podobno vlogo kot jo je imel ftp strežnik, ki je bil namenjen za odlaganje namestitvenih paketov. Razlika je v tem, da se v SVN repozitorij poleg različic namestitvenih paketov odlaga tudi dokumentacijo, izvorno kodo in testne datoteke.

GTZ-PROJEKT-SPREMEMBE-40 Ko je projekt pripravljen za namestitev (to naj se v fazi implementacije zgodi čim prej), izvajalec pripravi izdajo aplikacije in odloži/shrani namestitveni paket projekta na namenski strežnik SVN za hranjenje verzij. SVN strežnik pripravi naročnik, predstavnikom izvajalca dodeli pravice odlaganja in branja ter mrežni dostop. Povezava na SVN repozitorij uporablja protokol https. Izvajalec odlaga izdelke v SVN s pomočjo razvojnega orodja (če vsebuje podporo za protokol SVN) ali pa preko odjemalca, ki podpira protokol SVN (kot npr.: TortoiseSVN, https://osdn.net/projects/tortoisesvn/).

Vsebina in drevesna struktura imenikov SVN je prikazana v spodnji tabeli:

MJU-SVN drevesna struktura v0.12k						
SVN-root	*I. Nivo*	*II. Nivo*	*III. Nivo*	*IV. Nivo*	*V. Nivo*	*VI. Nivo*
<NazivNaročnika/ ProgramProjektov>						
	<Projekt>					
		<Aplikacija>				
			<db_poizvedbe>			
				<log>		
				<sql>		
			<trunk>			
				<dokumentacija>		
					<OVSP>	
					<uporabniska>	
					<tehnicna>	
					<namestitvena>	
					<testna>	
				<app_objekti>		
					<build>	
					<config>	
					<deploy>	
					<resources>	
						<lib>
					<src>	
						<sklop 1>
						<sklop 2>
						...
					<kriticni_popravki>	
						<"datum"_"ura">
				<bazni_objekti>		
					<dba>	
						<info>
						<log>
					<src>	
					<deploy>	
					<kriticni_popravki>	
						<"datum"_"ura">
			<tags>			
				<verzija 1>		
				<verzija 2>		
				...		
			<SoC>			
				<Reports>		
				Manifest.MF		

Tabela 1. Okvirna vsebina drevesne strukture in pomen imenikov (Dejanska struktura se nahaja v prilogi dokumenta »Navodila za obvladovanje sprememb v SVN okolju«).



Slika 2. prikazuje okvirni princip sistema za obvladovanje sprememb, ki vsebuje repozitorij izvorne kode SVN (Subversion) ter orodje za izvajanje upravljanja ter izdelavo poročil (Jenkins) v povezavi s simbolično prikazano več nivojsko strežniško testno in produkcijsko infrastrukturo.

1.9 Vsebina dokumentacije in napotki za izdelavo

GTZ-PROJEKT-DOKUMENTACIJA-10 Izvajalec izdela, vzdržuje in odloži v repozitorij SVN dokumentacijo, ki vsebuje:

1. Dokumente OVSP postopka ter seznam celotne dokumentacije s kratkim opisom vsebine, navedbo celotnega imena datoteke, verzijo, lokacijo datoteke v imeniški strukturi in skupino v katero se dokumentacija uvršča.
2. Uporabniško dokumentacijo – navodila za uporabo za vse nivoje uporabnikov.
3. Načrt testiranja, testni postopki in testni podatki ter poročila o testiranju.
4. Seznam zunanjih orodij, ki niso del sistema in so potrebna za upravljanje in/ali razvoj sistema.
5. Dokumentacijo izvedene analize rešitve (t.i. sistemska analiza).
6. Dokumentacijo o arhitekturi in zasnovi sistema.
7. Podrobno tehnično dokumentacijo, ki praviloma zajema:

   7.1. standardno dokumentacijo izvorne kode,

7.2. dokumentacijo shem XML,
7.3. dokumentacijo vmesnikov spletnih storitev,
7.4. dokumentacijo programskih vmesnikov,
7.5. dokumentacijo uporabljenih lastnih ali tujih programskih komponent,
7.6. dokumentacijo postopkov in algoritmov, kar vključuje delovne tokove in vgrajena poslovna pravila,
7.7. splošno namestitveno shemo in navodila za namestitev v ciljno okolje za vsa podprta okolja,
7.8. diagram odvisnosti med programskimi vmesniki in sistemi.

8. Dokumentacijo o sistemskih nastavitvah za vse elemente sistema (podatkovna baza, aplikacijski strežnik, idr.) z opisom razlogov za spremembo privzete nastavitve.
   Opomba: *Ta točka je vsebinsko lahko pokrita tudi v navodilih za namestitev.*

GTZ-PROJEKT-DOKUMENTACIJA-20 Splošne zahteve glede izdelave in vsebine dokumentacije:

a) kjer se pojavljajo seznami datotek le-te dopolniti z opisi vsebine datotek in lokacijo datotek,

b) vse dokumente opremiti z verzijo dokumenta, verzijo programske komponente, ki jo dokument opisuje ali naslavlja, povezave na druge dokumente in opis sprememb dokumenta (datum, verzija dokumenta, avtor spremembe, opis spremembe, odgovorna oseba - opcijsko, kjer je to smiselno),

c) dokumentacija mora vsebovati seznam kratic in akronimov (v posameznih dokumentih ali kot ločen dokument),

d) v dokumentaciji je potrebno zagotoviti natančnost izražanja, dosledno podati verzije standardov in specifikacij, jasno je potrebno določiti podlago in izvor uporabljenih notacij (npr. za diagrame opredeliti po kateri notaciji so narisani, katera verzija, uporabljeno orodje, ipd.). Vsi diagrami in slike morajo biti ustrezno komentirani. Diagrami stanj morajo biti opremljeni z besednimi opisi,

e) Programsko kodo, sheme XML, datoteke HTML, definicije WSDL in druge elemente sistema, na podlagi katerih nastane izvedljiva in z njo povezana programska koda je potrebno dokumentirati skladno s standardi, dobrimi praksami in priporočili stroke.

f) programska in druga izvorna koda (XML, HTML, WSDL, SQL, slike in drugo multimedijsko gradivo, projektne datoteke za posamezne izdelke npr. datoteka .pom za projekte narejene v razvojnih orodjih, izvorne datoteke diagramov, idr.) z navedbo uporabljenih orodij vključno z verzijo.

1.10 Optimalnost aplikacije in baznih objektov

GTZ-OPTIMIZACIJA-SPL-10 Izvajalec je dolžan optimizirati programsko kodo in bazne objekte s ciljem zagotavljanja optimalnega delovanja. Vse neoptimalnosti, ki se izkažejo skozi obremenitveni test in skozi generalni preizkus mora izvajalec odpraviti do trenutka produkcije. Enako pravilo velja tudi za obdobje garancije oziroma obdobje operativnega vzdrževanja.

GTZ-OPTIMIZACIJA-SPL-11 Optimalno delovanje sistema je odvisno tudi od obsega podatkovne zbirke. Zato mora informacijski sistem vsebovati tudi procedure za periodični umik podatkov iz produkcijske podatkovne zbirke (zbirk).

GTZ-OPTIMIZACIJA-SPL-20 Prav tako mora izvajalec vsako spremembo ali nadgradnjo aplikacije predhodno preveriti tudi s performančnega stališča.

GTZ-OPTIMIZACIJA-SPL-30 Upravitelj infrastrukture izvaja periodične preglede optimalnega delovanja. Priporočila, ki nastanejo na podlagi takih pregledov je izvajalec dolžan v najkrajšem še razumnem roku upoštevati.

GTZ-OPTIMIZACIJA-SPL-40 Izvajalec mora obvladovati nivo SQL poizvedb (SQL poizvedbe ne smejo biti generirane na tak način, da jih izvajalec ne bi mogel popraviti, prilagoditi, optimizirati ali v celoti predrugačiti).

1.11 Namestitvena pravila

GTZ-POSTAVITVE-TUP-10 Za vsak modul/aplikacijo upravljavec infrastrukture vzpostavi okolja (testno, produkcijsko in v kolikor je potrebno šolsko/uvajalno) kot sledi:

I. testno okolje služi potrditvenemu testiranju (torej preverjanju, ali je bil nek popravek izveden v skladu z željami naročnika (samo regresijsko testiranje pravilnosti kode se izvaja na strani izvajalca);
II. produkcijsko služi polni produkciji. Sem se nameščajo samo popravki, katerih prehod iz testa na produkcijo je bil po predpisanem protokolu odobren. Prenos namestitve aplikacije ali njenih popravkov iz razvojnega preko testnega do produkcijskega definira t.i. RTP navodilo (Razvoj-Test-Produkcija). Podrobnejši način izvajanja navodila se določi prilagojeno značilnostim vsakega projekta posebej.,
III. uvajalno okolje je namenjeno izobraževanju uporabnikov (preverjanju delovanja integracij z zunanjimi sistemi) in naj bi bilo po verzijah aplikacij izenačeno s produkcijskim. Vzpostavljanje uvajalnega okolja se ne uvaja tam, kjer naročnik in upravljavec infrastrukture ocenita, da le-to ni potrebno (manjši oz manj kompleksni sistemi z malo spremembami ter malo uporabniki)

V primerih, ko to narava sistema zahteva, se lahko v dogovoru z naročnikom in upraviteljem infrastrukture vzpostavijo še dodatna okolja (npr predprodukcijsko…).

GTZ-POSTAVITVE-TUP-20 Za vsako namestitev novega modula ali popravka obstoječega modula mora izvajalec pripraviti ustrezna navodila za namestitev.

GTZ-POSTAVITVE-TUP-30
Podrobnosti postavitev okolij, ki so potrebna za dosego točke GTZ-STANDARDI-DEV-10 (zagotovitev procesa sestavljanja aplikacije iz izvorne kode) se dorečejo v okviru dokumenta PZI (odlaganje kode v SVN, verzije ciljnih izvajalnih okolij, oblike namestitvenih paketov, način podpore procesu prevajanja in nameščanja (ročni, avtomatski, kombinirani, oboje) etc).

GTZ-NAMESTITVE-RTP-10 Nove verzije/popravki tako spletnih aplikacij kot baznih objektov se najprej namestijo na testno področje;
Odgovorni predstavnik izvajalca opravi najmanj naslednja preverjanja:

I. da je bila namestitev opravljena v skladu s izvajalčevimi navodili,
II. da je aplikacija deluje v skladu s funkcionalnimi pričakovanji,
III. da je aplikacija tudi performančno ustrezna in deluje v skladu s pričakovanji;

GTZ-NAMESTITVE-RTP-20 Šele na podlagi pozitivnega izida tega potrditvenega testa, izjave odgovornega, da je bil test pozitivno opravljen, se lahko namesti namestitvena datoteka ali popravki na produkcijo.

GTZ-NAMESTITVE-RTP-30 Po namestitvi na produkcijo, izvajalec preveri delovanje po enakem vzoru, kot je bila narejena verifikacija na testu:

I. da odgovorni predstavnik izvajalca izvede potrditveni test na produkciji, ki sestoji najmanj iz naslednjega preverjanja:
II. da je bila namestitev opravljena v skladu z izvajalčevimi navodili,
III. da je aplikacija deluje v skladu s funkcionalnimi pričakovanji,
IV. da je aplikacija tudi performančno ustrezna in deluje v skladu s pričakovanji;

Potrditveni test mora obsegati poleg delovanja same aplikacije tudi delovanje podatkovne zbirke in ustreznost baznih objektov.

GTZ-NAMESTITVE-RTP-40 Nameščanje aplikacij in njih popravkov se izvaja v skladu s t.i. RTP navodilom Ministrstva za javno upravo (navodilo obravnava postopke obvladovanja sprememb Razvojnega, Testnega in Produkcijskega okolja) ter obrazcem OVSP.

GTZ-NAMESTITVE-RTP-50 Razvojno okolje (in testna okolja za razvojno testiranje) je na strani izvajalca.

GTZ-NAMESTITVE-RTP-60 Pri izvedbi projekta mora izbrani izvajalec tako upoštevati naslednjo dokumentacijo:

1) RTP pravilo oziroma politika (Priloga 1) in
2) Zahteve in obrazci za potrebe naročil za namestitev aplikacije/popravka (Priloga 2)

1.12 Obremenitveni test

GTZ-TESTI-OBREMENITVENI-10 Za kritične aplikacije ali celotni sistem, lahko naročnik zahteva izvedbo obremenitvenega preizkusa. Obremenitveni preizkus se običajno izvaja skupaj s strokovnjaki MJU/DI s pomočjo orodja JMeter. Izvajalec je dolžan pripraviti scenarije in podatke za to orodje. Naročnik si pridržuje pravico spremembe orodja za izvajanje obremenitvenih preizkusov.

1.13 Generalni preizkus

GTZ-TESTI-GENERALNI-10 Za kritične aplikacije z lahko določi naročnik izvedbo generalnega preizkusa. Generalni preizkus pomeni hkratno vajo vseh uporabnikov, njegov namen pa je preizkusiti tako sistem v simulaciji realne rabe, kot organizacijsko in tehnično okolje, v katerem sistem teče (kako dobro so obveščeni uporabniki, ali se uporabniki znajo prijaviti, ali točke podpore funkcionirajo primerno, ali obstajajo kje kake nepredvidene skrite ovire (npr slaba mrežna povezava na eni od lokacij/postaj). Lahko se izvaja tudi kot vzporedni test. Za generalni preizkus je izvajalec dolžan pripraviti vsebinske in postopkovne scenarije.

1.14 Statistični podatki in osnovna poročila

GTZ-NADZOR-STAT-10 Informacijska rešitev, ki je predmet javnega naročila mora omogočati izdelavo osnovnih statističnih poročil za podatke, ki so pomembni za upravljanje informacijske rešitve (kot na primer: statistika obiska, statistika postopkov (napak, po statusih), statistika po uporabi storitev, statistika urednikovanja ipd).

Statistične obdelave ne smejo negativno vplivati na delovanje transakcijskega dela sistema .

1.15 Nadzorni podatki

GTZ-NADZOR-SPL-10 Sistem naj nudi nadzorne konzole tako za sistemske kot za vsebinske upravljavce. Namen konzol je spremljanje delovanja, alarmiranje in zgodnje obveščanje, ter hitra identifikacija težav.

1.16 Nadzorni podatki: sistemsko / aplikacijski nivo

GTZ-NADZOR-SYS-10 Vsak od modulov naj nudi informacijo o statusu delovanja (deluje | ne deluje (opis napake)).

GTZ-NADZOR-SYS-21 Sistem mora zagotavljati metode, ki omogočajo sistemsko preverjanje osnovnega delovanja modula (tipičen primer take metode je neka funkcija, jsp datoteka, WSDL

metoda, ki izvede klic na bazo in vrne npr. datum.) Točen način implementacije se dogovori z upravljavcem infrastrukture v času razvoja kode pred prehodom sistema v produkcijo.

GTZ-NADZOR-SYS-22 Sistem mora tudi zagotavljati metodo, ki jo periodično naslavlja oprema za porazdeljevanje bremen oziroma failover (content switch oprema, load balancer, reverse proxy etc), tako, da zagotavlja informacijo o 'zdravju' dotične instance, inštalacije, modula.

GTZ-NADZOR-SYS-23 Sistem mora vsebovati (izdelane, oblikovno skladne html-je) spletne strani, ki so namenjene obveščanju uporabnikov ob morebitnih izpadih delovanja posamičnih komponent in ali celotnega sistema. Te strani se delijo na tri področja:

- stran z obvestilom o tem, da je sistem delno neoperativen zaradi vzdrževanja (ne deluje podsistem),
- stran, ki sporoča uporabniku, da je pri določeni operaciji prišlo do napake (obvladovanje napak na način, da aplikacijski strežnik ne sporoča internih podatkov),
- stran z obvestilom, ki sporoča, da je prišlo do večje tehnične napake in da je sistem neoperativen (sorry page).

GTZ-NADZOR-SYS-30

Sistem mora upravljalcu infrastrukture omogočati avtomatski nadzor nad delovanjem informacijskega sistema, ki se nad sistemom izvaja periodično (npr.: 5 minut).
Za potrebe avtomatskega preverjanja mora sistem nuditi testne metode, ki podajo osnovni status delovanja vsakega od samostojnih modulov sistema.
Omenjene metode naj ne pokrivajo testiranja do centralnih storitev infrastrukture, saj se le te, testirajo ločeno.
Optimalna izvedba te konzole oziroma celotnega sistema alarmiranja je stvar dogovora med naročnikom in izvajalcem in potrjena na nivoju PZI. Prvi predlog naj po izvedeni analizi poda izvajalec.

GTZ-NADZOR-SYS-35

Zahteva velja za sisteme, katerih delovanje je odvisno od integracij na vire ali storitve.

Sistem naj upravljavcu infrastrukture omogoča hiter pregled preko GUI vmesnika oziroma diagnosticiranje v primeru težav pri delovanju sistema **in** njegove umestitve v tehnološko okolje, v katerem teče.
Ta funkcionalnost ni namenjena za avtomatsko periodično testiranje ampak za primere diagnosticiranja ustreznosti namestitve ter, v času obratovanja sistema, hitre diagnostike težav.
Namen tega nadzornega elementa je testiranje dostopnosti virov s stališča/zornega kota dotičnega sistema: ali dotični sistem ima mrežno dostopnost do svojih virov, ali ima dotični sistem prave avtentikacijske parametre, ali ciljni sistem/vir obravnava te identifikacijske parametre po pričakovanjih (ali je možno vzpostaviti sejo, ali ima sistem pravice za klic ciljne storitve, …), etc. Pogled administratorja na tako nadzorno konzolo pokaže seznam vseh okolij/vej, na katerih so moduli nameščeni in na vsakem izmed okolij, seznam vseh modulov iz katerih je sistem sestavljen. Za vsak modul iz seznama se prikaže seznam vseh virov skupaj z indikatorjem uspešnosti ali neuspešnosti dostopa, ter v primeru napake, izpisom le te kolikor natančno jo je moč določiti. V seznamu navedeni viri se prikažejo kot dejanski naslovi klicev (URI, JNDI ime strežniškega vira, etc).
Primer: Modul, ki za svoje delovanje potrebuje več virov naj tudi nudi preverjanje delovanja oziroma dostopnosti do teh virov (če npr. za svoje delovanje modul potrebuje dostop do 3 podatkovnih virov (data source) ter 4 spletnih storitev, bo njegova nadzorna stran imela vsaj 8 tako imenovanih grafičnih simbolov - »semaforčkov«, en za modul sam po sebi, ostalih 7 za klicane vire. Pri tem naj vsak »semaforček« poda informacijo o napaki tako natančno, kolikor je to mogoče – npr. »časovna pretečenost« ali »napačni prijavni podatki«… Na zaslon se izpiše tako napaka, ugotovljena s strani klicočega modula kot napaka, ki smo jo morda pridobili iz klicanega modula).
Podobni obstoječi centralni nadzorni sistemi, na sistemskem nivoju informacijsko komunikacijske infrastrukture, ne nadomeščajo opisane funkcije.
Glede na to, da so podatki, ki jih posreduje nadzorna konzola interne narave, mora biti stran nadzorne konzole pod avtentikacijo, pooblastila za dostop do nadzorne konzole pa imajo sistemski in aplikativni skrbniki.

Optimalna izvedba in podrobnosti implementacije te konzole oziroma celotnega sistema alarmiranja je stvar dogovora med naročnikom in izvajalcem in potrjena na nivoju PZI. Prvi predlog naj po izvedeni analizi poda izvajalec.

GTZ-NADZOR-LOG-10 Koncept aplikativnega logiranja sistema mora biti zasnovan tako, da se lahko nastavlja nivo podrobnosti logiranja (informacije, opozorila, podrobne napake – info, debug, warn, error). Aplikativno logiranje (torej logiranje aplikativnih dogodkov) se ne beleži v transakcijsko podatkovno zbirko.
O izvedbi načina beleženja se natančneje dogovorita upravljavec infrastrukture ter izvajalec na nivoju PZI dokumentacije ali druge projektne dokumentacije.

1.17 Nadzorni podatki: vsebinski nivo

GTZ-NADZOR-PROCESI-10 Sistem mora nuditi pregled nad delovnimi tokovi, storitvami in drugimi dogodki (npr. dokument ali delovni tok stoji zaradi napake (tehnične, vsebinske ali druge)).
Zahteva velja za sisteme, ki implementirajo večstopenjske netrivialne procese.
GTZ-NADZOR-DOKUMENTI-10 Pregled nad potujočimi dokumentom oz. sporočili naj omogoča brskanje po dokumentih glede na njihove atribute (prioriteta, vir, ponor, tip ali drugo) brez potrebe po direktni prijavi v podatkovno zbirko z razvojnim orodjem.

1.18 Revizijske sledi

GTZ-NADZOR-REVIZIJA-10 Informacijska rešitev, ki je predmet javnega naročila mora zagotoviti v delih, kjer se obdelujejo osebni podatki ali finančni podatki ali podatki varnostnih shem (pravic dostopa) ustrezne revizijske sledi (dnevniki/journali).
Revizijske sledi morajo biti po vsebini, hrambi in sistemu nadzora (skupaj z varnostno shemo in povezanimi postopki) ustrezne, tako da zdržijo kot dokazni material pred pravosodnimi organi.

GTZ-NADZOR-REVIZIJA-20 Informacijski rešitvi mora izvajalec zagotoviti tudi pripadajoča orodja/preglede/poročila za obravnavo in interpretacijo revizijskih sledi.

GTZ-NADZOR-REVIZIJA-30 Izvajalec je dolžan upoštevati dobre prakse in priročnike objavljene na spletni strani Informacijske pooblaščenke glede na področja obdelave osebnih podatkov, še posebej priporočila v zvezi z varstvom osebnih podatkov pri povezovanju zbirk osebnih podatkov v javni upravi: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Varstvo_osebnih_podatkov_pri_povezovanju_zbirk_osebnih_podatkov_v_javni_upravi.pdf

1.19 Informacijska varnost in skladnost z zakonodajo

GTZ-VARNOST-PRAKSE-10 Informacijska rešitev, ki je predmet javnega naročila, mora biti izdelana z upoštevanjem Uredbe o informacijski varnosti v državni upravi (http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED7198) ter vseh dobrih praks in ustreznih rešitev, ki zagotavljajo visoko stopnjo informacijske varnosti. Rešitev ne sme imeti ranljivosti po OWASP TOP 10 seznamu, kjer so navedene najpogostejše napake spletnih aplikacij. Testiranje se lahko izvede ročno ali z avtomatskimi orodji. V primeru, da so bili testi izvedeni, je potrebno o tem predložiti tudi rezultate testiranja in v primeru pomanjkljivosti seznam teh in potrdilo o odpravi.
Informacijska rešitev, ki je predmet tega naročila, mora pred prvo produkcijo uspešno prestati preverjanje ranljivosti po OWASP TOP 10; vse morebitne odkrite pomanjkljivosti mora izvajalec odpraviti pred začetkom produkcije.
Upravljavec infrastrukture lahko ponovno preverjanje od izvajalca zahteva kadarkoli kasneje v življenjskem ciklu sistema. Izvajalec mora pomanjkljivosti, ugotovljene bodisi z uporabo orodja za testiranje bodisi ob praktični uporabi, odpraviti.

GTZ-VARNOST-NORMATIVI-10 Informacijski sistem mora biti skladen s področno zakonodajo, ki obravnava podatke, ki se obdelujejo v informacijskem sistemu skladno z namenom, načinom obdelave in stopnjo tveganja. Sistem je lahko predmet varnostnih pregledov, zato morajo biti pripravljene podlage, da se taki pregldi lahko izvedejo v najkrajšem možnem času.

GTZ-VARNOST-NORMATIVI-20 Rešitev ne sme ovirati naročnika pri prizadevanjih za približanje standardom ISO 27001 in 27002 v poglavjih, ki se nanašajo/navezujejo na informacijsko varnost in revizijske sledi.

GTZ-VARNOST-TESTI-10 Upravitelj infrastrukture podvrže sistem varnostnim testiranjem – preverjanje izvorne kode. Preverjanje izvorne kode (z orodjem Checkmarx) se začnejo izvajati takoj, ko izvajalno podjetje v SVN dostavi prve namestitve verzije, zato da se morebitne neskladnosti ali varnostne pomanjkljivosti odkrijejo zgodaj v razvojnem ciklu. Izvajalec je odkrite ranljivosti dolžan odpraviti v najkrajšem možnem času.

GTZ-VARNOST-TESTI-20 Upravitelj infrastrukture podvrže sistem varnostnim testiranjem (penetration testing) po postavitvi v testno okolje naročnika. Testiranje se izvede na zahtevo, po uspešno opravljeni namestitvi, njenem preizkusu delovanja, opravljenem funkcionalnem testiranju in pripravljenih ustreznih skrbniških/uporabniških računih za delo z aplikacijo. Pogoj je poročilo o opravljenem funkcionalnem testiranju v okolju naročnika.

Izvajalec je odkrite ranljivosti dolžan odpraviti v najkrajšem možnem času. Pred odpravo odkritih pomanjkljivosti/ranljivosti sistema prehod v produkcijo ni možen.

GTZ-VARNOST-OSEBNI-PODATKI-10 Informacijski sistem v katerem se obdelujejo osebni podatki, mora biti skladen s področno zakonodajo, ki obravnava podatke, ki se obdelujejo v informacijskem sistemu skladno z namenom, načinom obdelave in stopnjo tveganja.
Sistem, ki obdeluje osebne podatke, mora omogočati naročniku in Ministrstvu za javno upravo, ki je v vlogi upravljavca informacijske infrastrukture, izpolnjevanje zahtev predpisov, ki urejajo varstvo osebnih podatkov, vključno z določili Splošne uredbe o varstvu podatkov (Uredba (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA, z dne 27. aprila 2016, o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES), ki se začne neposredno uporabljati 25. 5. 2018.
Sistem je lahko predmet pregleda na izpolnjevanje skladnosti na področju obdelave osebnih podatkov, zato morajo biti pripravljene podlage, da se takšen pregled lahko izvede v najkrajšem možnem času. Izvajalec je odkrita neskladja, ki se nanašajo na funkcije predmetnega sistema dolžan odpraviti v razumnem roku.