



Generične Tehnološke Zahteve (GTZ) za razvoj informacijskih rešitev V 2.3.0

Oktober 2024

Kazalo vsebine

Generične Tehnološke Zahteve	1
1.0 Tehnološko okolje	5
1.1 Tehnološki standardi in specifikacije	6
1.2 Tehnološka neodvisnost na strani odjemalcev	6
1.3 Dokument PZI	7
1.4 Splošne arhitekturne smernice	8
1.5 Zahteve v zvezi s tehnologijo vsebnikov	8
1.6 Splošna postavitvena pravila	9
1.7 Način dostopa do podatkovne zbirke in obvladovanje sprememb nad podatki..	9
1.8 Metodologija razvoja ter upravljanje s spremembami programske opreme.....	10
1.9 Vsebina dokumentacije in napotki za izdelavo	11
1.10 Optimalnost aplikacije in baznih objektov	12
1.11 Namestitvena pravila	12
1.12 Obremenitveni preizkus.....	14
1.13 Generalni preizkus	14
1.14 Nadzorni podatki	14
1.15 Statistični podatki in osnovna poročila	15
1.1 Revizijske sledi	15
1.2 Informacijska varnost in skladnost z zakonodajo	15
Zgodovina sprememb dokumenta	17

O dokumentu:

Dokument je sestavljen iz serije zahtev¹, ki jih zastavlja tehnološko okolje, kamor se uvrščajo informacijske rešitve.

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 generične tehnološke zahteve

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 informacijske rešitve, ki so oz. bodo umeščeni na infrastrukturo MDP. Zahteve upravljalca infrastrukture predstavljajo obvezni del specifikacij predmetnega naročila.
Način upravljanja s spremembami	Z dokumentom upravlja MDP kot upravljalca infrastrukturnega okolja. MDP tudi izvaja spremembe nad dokumentom; tako se dokument v primeru upravičenih zahtev prilagodi na specifične razpisne dokumentacije za vsak razpis posebej.

Spremembe dokumenta		
28.2.2012 - 11.2.2021	1.0.1 - 2.2.9	Zgodovina sprememb dokumenta
17.10.2024	2.3.0	Spremembe: - sprememba MJU v MDP, - terminološki popravki zaradi poenotenja dokumentov s področja gostovanja na DRO, - GTZ-OKOLJE-SPL-10, dodan seznam podprtih tehnologij, ki se lahko uporabljajo v informacijski rešitvi, - GTZ-OKOLJE-SPL-20, odstranjena možnost nameščanja na fizične strežnike, - GTZ-OKOLJE-NIVOJI-10, dodan seznam Podprta programska oprema za delovanje informacijskih rešitev v okviru procesa gostovanja na Državnem računalniškem oblaku, - GTZ-OKOLJE-NIVOJI-20, razširitev podpore več izvajalnim okoljem, dodan seznam Podprta programska oprema za delovanje informacijskih rešitev v okviru procesa gostovanja na Državnem računalniškem oblaku, - GTZ-OKOLJE-NIVOJI-30, prilagojeno glede na širitev podpore več izvajalnim okoljem, - GTZ-OKOLJE-NIVOJI-40, dodan seznam Podprta programska oprema za delovanje informacijskih rešitev v okviru procesa gostovanja DRO, - GTZ-PROJEKT-PZI-30, črtano, - GTZ-VSEBNIKI-ENV-10, razširjena podpora na Kubernetes za tehnologijo vsebnikov nad Linux izvajalnim slojem, - GTZ-VSEBNIKI-ENV-20, razširitev za Kubernetes,

¹ V dokumentu se pojavljajo tudi deli besedila, ki niso neposredne zahteve za informacijske rešitve same po sebi, vendar pojasnjujejo okvir oz. gabarite, v okviru katere se informacijska rešitev umešča. Da informacijska rešitev ni v nasprotju s temi okviri, je zahteva. Primer: »Tehnološko okolje informacijske rešitve bo v celoti nameščeno na obstoječo infrastrukturo v upravljanju Ministrstva za digitalno preobrazbo (MDP). Predvidena je namestitvev na primarni lokaciji ter lokaciji nadomestnega centra (kolokacija).«

		- GTZ-VSEBNIKI-IMG-40, pri gradnji Docker slik se zasleduje koncept »Multi-stage builds«, - GTZ-VSEBNIKI-IMG-50, Datoteka dockerfile mora vsebovati metodo za preverjanje delovanja, t. i. HEALTHCHECK, - GTZ-BAZA-SPREMEMBE-10, dodana uporabo namenskih orodij za migracijo shem v relacijskih podatkovnih zbirkah, - GTZ-PROJEKT-SPREMEMBE-20, črtano - GTZ-PROJEKT-SPREMEMBE-25, črtano - GTZ-PROJEKT-SPREMEMBE-30, prilagojeno širitvi podpore na GIT repozitorij izvirne kode, - GTZ-PROJEKT-SPREMEMBE-40, črtano, - GTZ-PROJEKT-METODOLOGIJA-20, prilagojeno širitvi podpore na GIT repozitorij izvirne kode, - GTZ-PROJEKT-METODOLOGIJA-30, prilagojeno širitvi podpore na GIT repozitorij izvirne kode, - dopolnjeno poglavje 1.7. v delu obvladovanje sprememb nad podatki (dodano GTZ-BAZA-SPREMEMBE-10 in GTZ-BAZA-SPREMEMBE-20), - GTZ-PROJEKT-SPREMEMBE-10, dodan format MAJOR.MINOR.PATCH številčenja različic, - GTZ-PROJEKT-SPREMEMBE-20 in GTZ-PROJEKT-SPREMEMBE-25, črtano, - GTZ-PROJEKT-SPREMEMBE-30, prilagojeno širitvi podpore na GIT repozitorij izvirne kode, - GTZ-PROJEKT-SPREMEMBE-40, črtano, - GTZ-TESTI-OBREMENITVENI-10, dodana možnost, da obremenitveni preizkus lahko zahteva tudi upravljalec infrastrukture pred produkcijsko uporabo, - GTZ-TESTI-GENERALNI-10, dodano, generalni preizkus lahko zahteva pred produkcijsko uporabo tudi upravljalec infrastrukture, - dodano novo pravilo GTZ-VARNOST-PRAKSE-20 in dopolnjeno GTZ-PROJEKT-DOKUMENTACIJA-10 s točko 7.9. , - poglavja 1.15 Nadzorni podatki, 1.16 Nadzorni podatki: sistemsko/aplikacijski nivo, poglavje 1.17 Nadzorni podatki združena v poglavje 1.14. Nadzorni podatki in preoblikovano GTZ-NADZOR-SPL-10, črtano, GTZ-NADZOR-SYS-22, črtano, GTZ-NADZOR-SYS-30, črtano, GTZ-NADZOR-SYS-35, črtano, GTZ-NADZOR-PROCESI-10, črtano, GTZ-NADZOR-DOKUMENTI-10, črtano), GTZ-NADZOR-IR-10, dodano, - poglavje Statistični podatki in osnovna poročila preštevilčeno na 1.15, GTZ-NADZOR-STAT-10, črtano in nadomeščeno z GTZ-UPRAVLJANJE-10, - GTZ-NADZOR-LOG-10, dodano pravilo pisanja osebnih podatkov v dnevnike, - GTZ-VARNOST-PRAKSE-10, spremenjeno in dopolnjeno z ukrepi upravljalca infrastrukture v primeru neodprave pomanjkljivosti s strani naročnika, - GTZ-VARNOST-PRAKSE-20, dodane zahteve glede nesprejemljivosti uporabe »End-of-life« programske opreme in glede potrebe po vzdrževanju programske opreme v celotnem obdobju življenjske dobe informacijske rešitve, - GTZ-VARNOST-NORMATIVI-20, črtano, - GTZ-VARNOST-TESTI-10, črtano, - GTZ-VARNOST-TESTI-20, črtano.
--	--	---

1.0 Tehnološko okolje

GTZ-OKOLJE-SPL-10 Informacijska rešitev bo v celoti nameščena na obstoječo centralizirano infrastrukturo Državnega Računalniškega Oblaka (DRO) v upravljanju Ministrstva za digitalno preobrazbo (MDP). Seznam podprtih tehnologij, ki se lahko uporabljajo v informacijski rešitvi, je objavljen v ločenem dokumentu Podprta programska oprema za delovanje informacijskih rešitev v okviru procesa gostovanja informacijskih rešitev na Državnem računalniškem oblaku, ki je priloga GTZ, na [Portalu NIO](https://nio.gov.si) (<https://nio.gov.si>).

GTZ-OKOLJE-SPL-20 Glavne značilnosti infrastrukture DRO:

- na nivoju tehnološke infrastrukture:
 - a. infrastruktura zagotavlja visoko razpoložljivost, skalabilnost ter prenosljivost na različno strojno opremo,
 - b. informacijsko rešitev ali njene dele (module) se namešča prvenstveno v okolje vsebnikov,
 - c. za porazdelitev bremen se uporabi strojna ali programska oprema, 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 informacijske rešitve 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 informacijsko rešitev 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 želi upravljalec infrastrukture zagotoviti, da bo rešitev delovala na upravljalčevi obstoječi infrastrukturi. Upravljalec infrastruktur si pridržuje pravico do spremembe obstoječe tehnologije infrastrukture.

GTZ-OKOLJE-NEODV-20 Informacijske rešitve ne smejo biti zaklenjene na število procesorjev, količino spomina, velikost diska ali na kakršnekoli druge programske in strojne parametre.

GTZ-OKOLJE-NIVOJI-01 Informacijska rešitev 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 spletni strežnik.

GTZ-OKOLJE-NIVOJI-20 Za aplikacijski nivo informacijske rešitve je predvideno ciljno izvajalno okolje po specifikacijah programskega jezika.

Na razpolago so izvajalna okolja, ki so opredeljena v dokumentu Podprta programska oprema za delovanje informacijskih rešitev v okviru procesa gostovanja informacijskih rešitev na Državnem računalniškem oblaku, objavljen na [Portalu NIO](https://nio.gov.si) (<https://nio.gov.si>).

Uspešna namestitvev in uspešna izvedba funkcionalnih testov na testnem izvajalnem okolju je prva kontrolna točka v procesu implementacije informacijske rešitve na ciljno infrastrukturo.

Prva namestitvev na testno izvajalno okolje 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 (statični pregled izvorne kode).

GTZ-OKOLJE-NIVOJI-30

Upravljalca infrastrukture licenčno krije osnovno izvajalno okolje.

Tako v primeru Java, kot .NET in ostalih podprtih izvajalnih okolij se preferira uporaba tehnologije vsebnikov (docker)².

Upravljalca infrastrukture ne krije nobenih stroškov morebitnih dodatnih plačljivih tehnologij, storitev, ogrodi, aplikacij in drugih plačljivih dodatkov. Stroške za uporabo morebitnih plačljivih tehnologij, storitev, ogrodi, aplikacij in drugih plačljivih dodatkov nosi projekt in ne upravljalca infrastrukture, kar velja za ves čas življenjske dobe informacijske rešitve.

GTZ-OKOLJE-NIVOJI-40 Za podatkovni nivo je predvidena relacijska podatkovna zbirka, ki podpira standard SQL. Podprte tehnologije podatkovnih zbirk so navedene v dokumentu Podprta programska oprema za delovanje informacijskih rešitev v okviru procesa gostovanja informacijskih rešitev na Državnem računalniškem oblaku, objavljen na [Portal NIO \(https://nio.gov.si\)](https://nio.gov.si).

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 standardi³ in specifikacije pri razvoju spletnih rešitev.

GTZ-STANDARDI-SPL-20 Zahteve za IPv6 podporo v programski opremi. Vsa programska oprema, ki sestavlja informacijsko rešitev, 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 informacijske rešitve 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 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 MDP.

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 upravljalca 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 Edge, Mozilla Firefox, Chrome, Safari) odjemalca in operacijskih sistemov (npr. MS Windows, Linux, Mac OS) brez namestitvenih ali konfiguracijskih posegov na strani odjemalca, vključujoč brskalnik, operacijski sistem ali katerokoli komponento uporabniške delovne postaje.

² Glej poglavje 1.5.

³ 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.

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.⁴

1.3 Dokument PZI

GTZ-PROJEKT-PZI-10 Dokument Projekt za Izvedbo (PZI) je namenjen natančnemu popisu in specifikacijam bodoče informacijske rešitve (informacijskega sistema/aplikacije/modula). MDP 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 upravitelja centralne infrastrukture MDP, v primeru, da naročnik ni MDP.

MDP kot upravitelj 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 MDP optimizirati arhitekturo in implementacijo informacijske rešitve 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 se 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 informacijske rešitve.

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 nove informacijske rešitve oziroma večjih dograditev le-tega) ali drugi ustrezni projektni dokumentaciji (v primeru obstoječe informacijske rešitve).

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

- 1) Specifikacija poslovnih procesov, ki jih bo informacijska 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 informacijske rešitve 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 predmetnemu naročilu, kjer je za vsako zahtevo razvidno ali je implementacija zajeta v celoti ali pa so predvidena odstopanja s pripadajočo obrazložitvijo.

⁴ Primer: nabor relevantnih tehnologij bo torej lahko drugačen, če je razpisana informacijska rešitev namenjena uporabniški skupini referentov na upravnih enotah s standardiziranim delovnim okoljem, ali pa če je razpisana informacijska rešitev za najširši nabor internetnih uporabnikov – državljanov.

1.4 Splošne arhitekturne smernice

GTZ-ARHITEKTURA-NIVOJI-10 Arhitektura informacijske rešitve 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).

Informacijska rešitev, ki je predmet tega naročila mora delovati brez uporabe posebnih odjemalcev ali vtičnikov, razen ko tako eksplicitno določa naročnik v razpisni dokumentaciji.

GTZ-ARHITEKTURA-MODULARNOST-10 Informacijska rešitev mora biti zgrajena 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 upravljalcem infrastrukture (MDP) 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 Izvirne (začetne, FROM) docker slike morajo biti na voljo v javnih docker registrih (npr. Docker Hub) ter so predmet usklajevanja tekom pregleda PZI dokumentacije.

Izvirne 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 upravljalca 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 upravljalca infrastrukture. Datoteka dockerfile se smatra za del izvirne kode.

GTZ-VSEBNIKI-IMG-40 Pri gradnji Docker slik se zasleduje koncept »Multi-stage builds«.

GTZ-VSEBNIKI-IMG-50 Datoteka Dockerfile mora vsebovati metodo za preverjanje delovanja, t. i. HEALTHCHECK.

GTZ-VSEBNIKI-LOG-10 Za potrebe zbiranja in vpogleda v dnevnike vsebniških aplikacij je na centralni infrastrukturi postavljeno orodje OpenSearch (<https://opensearch.org>), 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 OpenSearch in logiranje na stdout.

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

GTZ-VSEBNIKI-ENV-10 Za orkestracijo se uporablja tehnologija vsebnikov Docker SWARM ali Kubernetes postavljena nad Linux izvajalnim slojem. Aplikacija ne sme biti odvisna od izbire orkestratorja. Posamezni servisi so znotraj aplikacije mrežno naslovljivi z imenom servisa.

GTZ-VSEBNIKI-ENV-20 Aplikacija je dolžna za shranjevanje gesel, ostalih skrivnosti in konfiguracij uporabljati za kontejnerje v skladu z dobro prakso:

- 1) skrivnosti (gesla, certifikati, ...): preko možnosti "Docker Secrets", "Kubernetes Secrets",
- 2) konfiguracije (razne konfiguracijske datoteke): preko možnosti "Docker Configs".

GTZ-VSEBNIKI-ENV-30: V grućah vsebnikov (Docker SWARM Cluster) sobiva već informacijskih rešitev. Poimenovanje posameznih mikrororitev (vsebniskih servisov) se doloći skupaj s sistemskimi ekipami upravljalca infrastrukture, pri ćemer imajo imena mikrororitev (servisov) za predpono ime informacijske rešitve (aplikacije).

GTZ-VSEBNIKI-ENV-40: Namešćanje sistemskih Docker komponent na virtualne strežnike, vzpostavitev Docker gruće in konfiguracija orkestratorja **NI** stvar aplikacije. Razvijalec naj predpostavi obstojeće v naprej pripravljeno izvajalno okolje, ki ga vzpostavi upravljalet infrastrukture.

1.6 Splošna postavitvena pravila⁵

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

GTZ-POSTAVITEV-CONE-20 Moduli, do katerih dostopajo izkljućno HKOM uporabniki, se namešćajo znotraj intraneta komunikacijskega omrežja državnih organov. Toćna postavitvev modulov se doloća, ko so znani gabariti posameznega modula (znaćilnost aplikacije, nabor uporabnikov, nivo zahtevane varnosti, prićakovane obremenitve ipd.) skupaj s strokovnjaki upravljalca infrastrukture.

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

GTZ-POSTAVITEV-PROXY-10 V primerih, ko informacijska rešitev dostopa do internetnih spletišč ali spletišč nekaterih pridruženih omrežjih, je za http(s) komunikacijo predpisana uporaba internega posrednika (proxy strežnik) z namenom enoznaćne predstavitve IP naslova. S tem se omogoća enostavna selitev/dodajanje aplikacije na drug strežnik.

Informacijska rešitev mora omogoćati dostop do ciljanih spletišč tako neposredno, kot posredno, kar se doloća v konfiguracyjski datoteki (GTZ-POSTAVITEV-CONFIG-10).

1.7 Naćin dostopa do podatkovne zbirke in obvladovanje sprememb nad podatki

GTZ-BAZA-DOSTOP-10 Zahteva upravljalca infrastrukture je, da se aplikacija/modul na bazo prijavlja z računom (account/uporabnik) s tistim minimalnim naborom pravic, ki aplikaciji še omogoća delovanje oziroma izvrševanje poslovnih funkcij, ki jih aplikacija implementira.

V nadaljevanju je zahteva pod to oznako spisana v terminologiji Oracle podatkovnih zbirk. V primeru, da informacijska rešitev uporablja 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 ipd.). 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.

⁵ V primeru docker aplikacij glej tudi GTZ-VSEBNIKI-ENV-*

Bazni uporabnik, namenjen prijavi na bazo, se ustvari za vsak samostojen modul aplikacije/sistema posebej (npr. : modul portal, modul spletne storitve, modul za administracijo...) ⁶

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, 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 ipd.

GTZ-BAZA-DOSTOP-30 Izjema za pravilo *GTZ-BAZA-DOSTOP-20* je bralni način dostopa do šifrantov in klasifikacij ter list vrednosti, 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 upraviteljem infrastrukture v okviru PZI, pri čemer se tehta med vložkom v razvoj, predvidenimi stroški vzdrževanja (razvojni vidik, sistemski vidik), morebitnimi specifičnimi lastnostmi sistema ali posameznih transakcij v okviru tega sistema, izkušnjami sistemskih in razvojnih ekip ter drugimi dejavniki, ki so znani v času sestavljanja PZI.

GTZ-BAZA-SPREMEMBE-10 Obvladovanje sprememb podatkovnega modela in podrejenih podatkovnih procedur se izvaja preko DDL (Data Definition Language) skript, ki se posredujejo in verzionirajo preko repozitorija izvirne kode ali z uporabo namenskih orodij za migracijo shem v relacijskih podatkovnih zbirkah.

GTZ-BAZA-SPREMEMBE-20 Spremembe podatkov se izvajajo izključno preko aplikativne rešitve informacijskega sistema.

1.8 Metodologija razvoja ter upravljanje s spremembami programske opreme

GTZ-PROJEKT-METODOLOGIJA-10 Upravitelj 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 Upravitelj infrastrukture pričakuje, da ima izvajalec vzpostavljen proces v okviru razvojne metodologije, ki izdelke razvoja hrani v repozitoriju izvirne kode (SVN (Sub)VersionControl, GIT ali primerljivo) ter da sproti izvaja teste (Unit testi).

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

⁶ Primer: sistem 'foobar' z enim administrativnim in enim vpogledovalnim modulom za javnost bi torej potreboval (vsaj) sledeče 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.

GTZ-PROJEKT-SPREMEMBE-10 Od izvajalca se pričakuje, da ima izdelane in uveljavljene postopke obvladovanja sprememb (repozitorij, številčenje različic). Za številčenje različic se uporablja MAJOR.MINOR.PATCH format (primer: 1.1.1).⁷ 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-30 Izdelki razvoja se posredujejo/odlagajo naročniku v namenski repozitorij izvorne kode - v predpisani strukturi. V repozitorij se poleg različic namestitvenih paketov odlaga tudi dokumentacija, izvorna koda in testne datoteke.

1.9 Vsebina dokumentacije in napotki za izdelavo

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

1. Dokumente 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 informacijske rešitve in so potrebna za upravljanje in/ali razvoj informacijske rešitve.
5. Dokumentacijo izvedene analize rešitve (t. i. sistemska analiza).
6. Dokumentacijo o arhitekturi in zasnovi informacijske rešitve.
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,
 - 7.9. seznam verzij sestavnih delov informacijske rešitve in izvajalnega okolja z roki podpore.
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.

⁷ MAJOR.MINOR.PATCH format:

- MAJOR predstavlja oznako nove verzije ali verzije z nezdružljivimi spremembami s predhodno verzijo,
- MINOR predstavlja oznako verzije z dodanimi funkcionalnostmi, ki so združljive s predhodno verzijo,
- PATCH predstavlja oznako verzije, ki odpravlja napake predhodne verzije.

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

- a) kjer se pojavljajo sezname 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 informacijske rešitve, 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 multimedijско 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 informacijske rešitve je odvisno tudi od obsega podatkovne zbirke. Zato mora informacijska rešitev 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 Upravljelec 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 predukačiti).

1.11 Namestitvena pravila

GTZ-POSTAVITVE-TUP-10 Za vsak modul/aplikacijo upravljelec 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 okolje 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 zunanji sistemi) in naj bi bilo po verzijah aplikacij izenačeno s produkcijskim. Vzpostavljanje uvajalnega okolja se ne uvaja tam, kjer naročnik in upravljalec infrastrukture ocenita, da le-to ni potrebno (manjši oz. manj kompleksni sistemi z malo spremembami ter malo uporabniki)
- V primerih, ko to narava informacijske rešitve zahteva, se lahko v dogovoru z naročnikom in upravljalcem infrastrukture vzpostavi 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 postavitve okolij, ki so potrebna za doseg točke GTZ-STANDARDI-DEV-10 (zagotovitev procesa sestavljanja aplikacije iz izvorne kode) se dorečejo v okviru dokumenta PZI (odlaganje kode v repozitorij izvorne kode, verzije ciljnih izvajalnih okolij, oblike namestitvenih paketov, način podpore procesu prevajanja in nameščanja (ročni, avtomatski, kombinirani, oboje) ipd.).

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 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 MDP (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 preizkus

GTZ-TESTI-OBREMENITVENI-10 Za kritične aplikacije ali celotni sistem, lahko naročnik zahteva izvedbo obremenitvenega preizkusa. Izvedbo obremenitvenega preizkusa lahko zahteva tudi upravljalec infrastrukture pred produkcijsko uporabo. Obremenitveni preizkus se običajno izvaja skupaj s strokovnjaki MDP s pomočjo orodja JMeter. Izvajalec je dolžan pripraviti scenarije in podatke za to orodje. Upravljalec infrastrukture si pridržuje pravico spremembe orodja za izvajanje obremenitvenih preizkusov.

1.13 Generalni preizkus

GTZ-TESTI-GENERALNI-10 Za kritične aplikacije lahko določi naročnik izvedbo generalnega preizkusa. Generalni preizkus, ki ga lahko zahteva pred produkcijsko uporabo tudi upravljalec infrastrukture, pomeni hkratno vajo vseh uporabnikov, njegov namen pa je preizkusiti tako informacijsko rešitev v simulaciji realne rabe, kot organizacijsko in tehnično okolje, v katerem informacijska rešitev 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 Nadzorni podatki

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

GTZ-NADZOR-SYS-21 Informacijska rešitev mora zagotavljati metode za sistemsko preverjanje 'zdravja' končnih točk. Način nadzora končnih točk naročnik dogovori z upravljavcem infrastrukture pred prehodom informacijske rešitve v produkcijo.

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

- stran z obvestilom o tem, da je informacijska rešitev delno neoperativna 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 informacijska rešitev neoperativna (sorry page).

GTZ-NADZOR-IR-10

- delovanje operacijskih sistemov podatkovnih zbirk in docker izvajalnega okolja je nadzorovano na nivoju infrastrukture,
- za nadzor delovanja vsebnikov je informacijsko rešitev možno vključiti v sistem prometheus grafana. Razvijalec pripravi definicijo nadzornih konzol (dashboardov),
- za primere rešitev, ki so odvisne od klicanih integracijskih točk (kjer informacijska rešitev kliče druge storitve), je priporočljivo, da ima informacijska rešitev vzpostavljeno možnost pregleda zdravja integracij ter proženja integracij na zahtevo,
- naročnik in sistemska ekipa se lahko dogovorita za drugo obliko nadzora.

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 upravljalec infrastrukture ter izvajalec na nivoju PZI dokumentacije ali druge projektne dokumentacije.

Osební podatki se ne pišejo v dnevniké, oziroma, če tako določi naročnik, le izjemoma ob potrebi po raziskavi napake. Pri tem naj bo nivo izpisa (DEBUG, TRACE) tako 'globok', da se ga v produkcijskem okolju v času normalne rabe ne uporablja. Izpis osebnega podatka z nivojem, ki je višji od opredeljenega, se obravnava kot napaka v aplikaciji, ki jo je potrebno nemudoma odpraviti.

1.15 Statistični podatki in osnovna poročila

GTZ-UPRAVLJANJE-10 Informacijska rešitev mora omogočati osnovne izpise in poročila, ki jih bo naročnik potreboval v življenjskem ciklu informacijske rešitve. Izvozi podatkov iz baz za te namene niso dovoljeni.

1.1 Revizijske sledi

GTZ-NADZOR-REVIZIJA-10 Informacijska rešitev mora zagotoviti v delih, kjer se obdelujejo osebni podatki ali finančni podatki ali podatki varnostnih shem (pravic dostopa) ustrezne revizijske sledi (dnevnik/journali).

Revizijske sledi morajo biti po vsebini, hrambi in sistemu nadzora (skupaj z varnostno shemo in povezanimi postopki) ustrezne, tako da zdrži 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

1.2 Informacijska varnost in skladnost z zakonodajo

GTZ-VARNOST-PRAKSE-10 Informacijska rešitev mora biti izdelana z upoštevanjem predpisov, ki urejajo področje informacijske varnosti ter vseh dobrih praks in ustreznih rešitev, ki zagotavljajo visoko stopnjo informacijske varnosti. Rešitev ne sme imeti ranljivosti po OWASP TOP 10 seznamu. Informacijska rešitev mora prestati vsa varnostna testiranja, ki so predpisana v postopku gostovanja, vse morebitne odkrite pomanjkljivosti mora naročnik odpraviti pred začetkom produkcijske uporabe.

Upravljalca infrastrukture lahko zahteva ponovno preverjanje od naročnika kadarkoli kasneje v življenjskem ciklu informacijske rešitve. Naročnik mora pomanjkljivosti odpraviti v čim krajšem možnem času. V primeru, da naročnik pomanjkljivosti ne odpravi, se lahko upravljalec infrastrukture posluži ustreznih, nujnih in sorazmernih ukrepov za zaščito centralnega informacijsko-komunikacijskega sistema. Ukrepi lahko vključujejo tudi začasni odklop varnostno neustrezne informacijske rešitve iz centralnega informacijsko-komunikacijskega sistema, dokler ugotovljene pomanjkljivosti niso odpravljene.

GTZ-VARNOST-PRAKSE-20 Informacijska rešitev, uporabljene knjižnice in tehnološko izvajalno okolje morajo temeljiti na podprti programski opremi. Uporaba »End-of-life« programske opreme, ki se ji je iztekla podpora (podpora proizvajalca, podpora skupnosti) v produkciji ni sprejemljiva, ker predstavlja varnostna tveganja. Planiranje rokov podpore posameznih sestavnih delov informacijske rešitve in izvajalnega okolja je potrebno načrtovati in spremljati v celotnem obdobju življenjske dobe informacijske rešitve. Dokumentacija se vodi v okviru GTZ-PROJEKT-DOKUMENTACIJA-10 (7.9).

GTZ-VARNOST-NORMATIVI-10 Informacijska rešitev mora biti skladna s področno zakonodajo, ki obravnava podatke, ki se obdelujejo v informacijski rešitvi skladno z namenom, načinom obdelave in stopnjo tveganja.

Informacijska rešitev je lahko predmet varnostnih pregledov, zato morajo biti pripravljene podlage, da se taki pregledi lahko izvedejo v najkrajšem možnem času.

GTZ-VARNOST-OSEBNI-PODATKI-10 Informacijska rešitev v kateri se obdelujejo osebni podatki, mora biti skladna s področno zakonodajo, ki obravnava podatke, ki jih obdeluje informacijska rešitev skladno z namenom, načinom obdelave in stopnjo tveganja.

Informacijska rešitev, ki obdeluje osebne podatke, mora omogočati naročniku in MDP, ki je v vlogi upravljalca informacijske infrastrukture, izpolnjevanje zahtev predpisov, ki urejajo varstvo osebnih podatkov.

Informacijska rešitev 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 predmetne informacijske rešitve, dolžan odpraviti v razumnem roku.

Zgodovina sprememb dokumenta

Zgodovina sprememb 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
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.
18.5.2016	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 zaželenih časovnice: zaradi uvedbe varnostnega testiranja z orodjem CheckMarx, ki ga je v razvojni cikel smiselno uvesti v čim zgodnejši fazi, zahteva GTZ-OKOLJE-NIVOJI-20 spodbuja k oddaji kode v ustrezen repozitorij v čim zgodnejši 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;
24.5.2017	2.2.4	Prilagoditev dikcije v zahtevi GTZ-VARNOST-NORMATIVI-20
1.9.2017	2.2.5	Prilagoditev dikcije v zahtevi <u>GTZ-VARNOST-NORMATIVI-10 pregled -> pregledi</u>
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
5.3.2018	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«
26.4.2018	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 <u>GTZ-STANDARDI-SPL-20</u>, - <u>sprememba GTZ-PROJEKT-PZI-11, namesto MJU potrdi, MJU uskladi,</u> - 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 <u>GTZ-PROJEKT-SPREMEMBE-40, posodobljen URL,</u> <u>posodobljena tabela strukture SVN.</u>