

TEHNIČNE SPECIFIKACIJE – tehnični del dokumentacije v zvezi z oddajo javnega naročila
za javno naročilo
»Uvedba okoljsko manj obremenjujoče e-hrambe«



1. PREDMET NAROČILA.....	2
2. SKLADNOST, VARNOST IN PRAVNI OKVIR.....	3
2.1. Zakonodajna skladnost	3
3. VZPOSTAVITEV CERTIFICIRANE E-HRAMBE ZA VEČ-ORGANIZACIJSKO OKOLJE	4
3.1. Splošne in funkcionalne zahteve za sistem e-hrambe	4
3.2. Arhitektura sistema.....	4
3.3. Hramba dokumentov, zaščita podatkov in varnostne kopije	4
3.4. Življenjski cikel gradiva, klasifikacija in uničenje	5
3.5. Verzije in revizijske sledi	5
3.6. Uvoz, izvoz in migracije.....	6
3.7. Integracije in API	6
3.8. Uporabniški vmesnik.....	6
3.9. Tipi dokumentov	6
3.10. Iskanje dokumentov.....	7
3.11. Avtentikacija in dostop	7
3.12. Upravljanje ranljivosti in posodobitev (Patch Management).....	8
3.13. Upravljanje sprememb (Change Management).....	9
3.14. Obravnava varnostnih incidentov.....	9
3.15. Življenjski cikel in podpora.....	10
3.16. Razpoložljivost in nadzor	10
3.17. Fizična in organizacijska varnost.....	10
3.18. Usposabljanje naročnikovih uporabnikov za uporabo sistema	11
3.19. Podrobnejši časovni načrt	11
4. PODPORA PRI VZPOSTAVITVI BREZŠIVNE INTEGRACIJE DOKUMENTNEGA SISTEMA BUSINESSCONNECT Z E-HRAMBO	11
5. PRETVORBA IN ENKRATNI UVOZ GRADIVA IZ RAZLIČNIH DATOTEK	11
5.1. Obseg in struktura dokumentarnega gradiva naročnika.....	11
5.1.1. Viri dokumentacije	11
5.1.2. Formati datotek.....	11
5.1.3. Oblika in pretvorba dokumentacije	12
6. OCENJENE KOLIČINE GRADIVA IN LETNI PRIRAST	12
7. ELEKTRONSKA HRAMBA DOKUMENTACIJE S TEHNIČNO PODPORO	12
7.1. Upravljanje kadrovskih sprememb pri ponudniku	13

1. PREDMET NAROČILA

Dokumentacija v zvezi z oddajo javnega naročila – Uvedba e-hrambe



HSE je nosilec skupnega poslovnega procesa informacijske podpore za več družb skupine HSE (Dravske elektrarne Maribor d.o.o. (DEM), Soške elektrarne Nova Gorica d.o.o. (SENG), HSE INVEST d.o.o. (HSE INVEST) ter RGP d.o.o. (RGP), zato se storitve e-hrambe po tem javnem naročilu zagotavljajo tako HSE kot tudi navedenim odvisnim družbam (DEM, SENG, HSE INVEST in RGP).

Predmet javnega naročila je:

- vzpostavitev certificirane e-hrambe v oblaku izvajalca,
- pretvorba in uvoz gradiva iz datotek v e-hrambo,
- storitve elektronske hrambe gradiva in tehnična podpora za obdobje šestdeset (60) mesecev.

Podrobneje naročilo obsega naslednje vsebine:

1. Vzpostavitev certificirane e-hrambe za več-organizacijsko okolje za zgoraj navedene družbe iz skupine naročnika, v času trajanja pogodbe si naročnik pridržuje pravico vključiti v naročilo še dodatne družbe;
2. Podpora pri vzpostavitvi brezšivne integracije dokumentnega sistema BusinessConnect z e-hrambo;
3. Pretvorba in enkratni uvoz gradiva iz različnih datotek:
 - Zvočno gradivo;
 - Gradivo, ki ga bo iz fizičnega gradiva zajel zunanji izvajalec, ki je bil izbran za zajem gradiva. Gradivo bo v dogovorjeni strukturi, prav tako pretvorba s strani izbranega ponudnika e-hrambe ne bo potrebna;
 - Gradivo, izvoženo iz dokumentnega sistema ODOS.
4. Elektronska hramba dokumentacije s tehnično podporo za obdobje šestdeset (60) mesecev.

2. SKLADNOST, VARNOST IN PRAVNI OKVIR

2.1. Zakonodajna skladnost

Sistem e-hrambe, hramba in vse ostale storitve morajo biti v celoti skladne z:

- Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA, Uradni list RS, št. 30/06 s spremembami),
- Uredbo o varstvu dokumentarnega in arhivskega gradiva (Uradni list RS, št. 42/17),
- Direktivo (EU) 2022/2555 EVROPSKEGA PARLAMENTA IN SVETA z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114/ES (NIS2),
- Zakonom o informacijski varnosti (ZInfV-1, Uradni list RS, št. 40/25),
- Uredbo (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 (Splošna uredba o varstvu podatkov oziroma uredba GDPR),
- Zakonom o varstvu osebnih podatkov (ZVOP-2, Uradni list RS, št. 163/22, s spremembami),
- standardom ISO/IEC 27001:2022,
- dobrimi praksami (CIS Controls, NIST CSF),

oziroma z vsakokratno veljavnimi predpisi z zgoraj navedenih področij.

Ostalo, kar mora izbrani ponudnik v fazi izvedbe pogodbe zagotavljati:

- ponudnik mora v celotnem obdobju produkcijske uporabe sistema e-hrambe imeti veljaven certifikat za področje izvajanje storitev e-hrambe ISO 27018,
- ponudnik mora tekom trajanja javnega naročila zagotoviti redno presojo skladnosti sistema in svojih procesov (notranjo ali zunanjo revizijo, če je zahtevano),
- presoja skladnosti mora biti izvedena najmanj enkrat letno ali ob pomembnih spremembah sistema,
- v primeru neskladnosti mora ponudnik pripraviti načrt ukrepov z roki za odpravo ugotovljenih pomanjkljivosti,

Pripombe dodal [IK1]: Naročnik naj razmisli o vključitvi dodatnega zakona in sicer Zakon o varstvu osebnih podatkov (ZVOP-2).

Obrazložitev: Sistem e-hrambe bo zelo verjetno vseboval tudi osebne podatke zaposlenih, strank, poslovnih partnerjev ali drugih posameznikov, zato poleg neposredne uporabe uredbe GDPR predstavlja ZVOP-2 ključen nacionalni predpis za urejanje posebnosti obdelave osebnih podatkov v Republiki Sloveniji. ZVOP-2 dodatno opredeljuje področja, kot so videonadzor, obdelava osebnih podatkov zaposlenih, nadzor nad obdelavo ter pristojnosti nadzornega organa, kar je lahko relevantno tudi v kontekstu e-hrambe. Vključitev ZVOP-2 v zahteve zagotavlja celovitejšo pravno skladnost, zmanjšuje tveganje neskladnosti pri obdelavi osebnih podatkov ter jasno opredeljuje obveznosti ponudnika pri ravnanju z osebnimi podatki v okviru storitev e-hrambe.



- na zahtevo naročnika mora ponudnik omogočiti vpogled v dokazila o skladnosti (npr. certifikate, revizijska poročila, izjave o skladnosti).

3. VZPOSTAVITEV CERTIFICIRANE E-HRAMBE ZA VEČ-ORGANIZACIJSKO OKOLJE

3.1. Splošne in funkcionalne zahteve za sistem e-hrambe

Naročnikove splošne in funkcionalne zahteve so prikazane v tabeli Priloge 1 - Naročnikove zahteve za sistem e-hrambe.

Za izpolnjevanje tehnične ustreznosti ponujenega sistema e-hrambe morajo biti izpolnjene vse zahteve z DA.

3.2. Arhitektura sistema

Sistem e-hrambe mora biti ponujen kot certificirana storitev e-hrambe v oblaku:

- brez nameščanja strežniških komponent pri naročniku,
- z ločenim testnim in produkcijskim okoljem,
- z visoko razpoložljivostjo, geografsko redundanco in skalabilnostjo.

Podpora razpršenim repozitorijem in njihovi sinhronizaciji mora biti v celoti zagotovljena na strani ponudnika.

Sistem mora biti vzpostavljen:

- na najmanj dveh (2) aktivnih produkcijskih lokacijah, ki sta geografsko ločeni in nameščeni na potresno neodvisnih območjih,
- na tretji, ločeni offline lokaciji za hrambo varnostnih kopij, ki je fizično in logično ločena ter zaščiten pred sočasnim kompromitiranjem.

Izpad posamezne lokacije ne sme vplivati na dostopnost dokumentov.

Segmentacija omrežja in sistemska arhitektura:

- omrežje mora biti segmentirano v skladu s Purdue modelom (za OT okolja) oziroma po smiselno določenih varnostnih conah in nivojih (za IT okolja),
- vzpostavljene morajo biti jasne komunikacijske meje med posameznimi conami, podprte z usmerjevalniki, požarnimi in nadzornimi mehanizmi,
- neposredna komunikacija med OT in IT segmenti ni dovoljena, razen preko varnostno nadzorovanih prehodov (npr. DMZ, proxy, data diode, jump strežniki),
- nujno je ločevanje vsaj produkcijskega in testnega okolja, po potrebi tudi razvojnega, pri čemer testno okolje ne sme imeti dostopa do produkcijskih podatkov ali sistemov,
- vzpostavljeno testno okolje mora biti identično produkcijskemu okolju,
- prepovedan je neposreden dostop iz zunanjega interneta do notranjih sistemov,
- oddaljeno vzdrževanje je dovoljeno izključno preko varnih, avtoriziranih in nadzorovanih administrativnih kanalov (npr. VPN, ZTNA, PAM), brez "direct inbound" povezav iz interneta,
- za vse povezave mora biti zagotovljena dvofaktorska avtentikacija in beleženje vseh administratorskih sej,
- dostop dobaviteljev do naročnikovih dokumentov in vsebin je dovoljen samo v omejenem časovnem obdobju, na podlagi vnaprej odobrenega postopka naročnikove službe za informacijsko varnost, z beleženjem aktivnosti,
- topologija in segmentacija omrežja se morata redno pregledovati in posodabljeni, zlasti ob spremembah v infrastrukturi ali integraciji novih sistemov.

Omogočena mora biti več-organizacijska arhitektura. Podatki morajo biti ločeni glede na pravno osebo (hčerinske družbe) znotraj istega sistema e-hrambe.

3.3. Hramba dokumentov, zaščita podatkov in varnostne kopije



Sistem mora uporabljati mehanizem deduplikacije podatkov, kot je npr. »Single Instance Storage«, ali enakovredno tehnologijo, s katero se zagotovi, da so identične vsebine v e-hrambi shranjene fizično samo enkrat, ne glede na število arhivskih zapisov ali uporabnikov.

Zahtevana je ločitev:

- metapodatkov (v podatkovni bazi),
- dokumentov (Blob) izven podatkovne baze, pri čemer neposreden dostop do dokumentov mimo aplikacijskega sloja ni dovoljen.

Vsi dokumenti morajo biti dostopni izključno prek aplikacije, brez neposrednih URL-jev.

Šifriranje in zaščita podatkov:

- vsi podatki morajo biti šifrirani:
 - o pri prenosu: z uporabo TLS 1.2 ali novejšega,
 - o v mirovanju: z uporabo AES-256 ali drugega kriptografskega algoritma enakovredne varnostne ravni.
- če ponudnik uporablja javne oblake, certifikate ali zunanje ponudnike storitev, morajo biti ti skladni z mednarodnimi varnostnimi standardi, kot so ISO/IEC 27017 in ISO/IEC 27018,
- vsi podatki v zvezi z izvedbo storitve e-hrambe, vključno z varnostnimi kopijami, DR mehanizmi in dnevniki (logi) se morajo hraniti na ozemlju Republike Slovenije,
- strogo prepovedan je izvoz ali kakršnakoli obdelava podatkov naročnika izven Republike Slovenije,
- sistem mora omogočati razvrščanje po stopnji občutljivosti (npr. javni, interni, zaupni, strogo zaupni) in zaščito v skladu z določenim razredom varovanja,
- ključi za šifriranje morajo biti varno shranjeni in upravljeni (npr. z uporabo HSM ali Key Vault rešitev), dostop pa dovoljen samo pooblaščenim osebam,
- ponudnik mora zagotoviti, da je uporabljena kriptografija skladna z vsakokratno aktualnimi priporočili ENISA in da se ne uporabljajo zastareli ali ranljivi algoritmi.

Varnostne kopije:

- vsi podatki morajo biti redno varnostno kopirani, najmanj enkrat dnevno,
- varnostna kopija (backup) mora biti fizično in logično ločena od primarnega sistema ter zaščiten pred nepooblaščenimi spremembami ali brisanjem (npr. z WORM, immutable ali drugimi tehnično enakovrednimi mehanizmi),
- test obnavljanja backup-ov mora biti izveden najmanj enkrat letno,
- ponudnik mora imeti dokumentiran in preizkušen Disaster Recovery plan (DRP) z določenimi RTO/RPO vrednostmi,
- za kritične produkcijske sisteme je treba predvideti geo-redundanco ali replikacijo podatkov in visoko razpoložljivost že v fazi načrtovanja rešitve.

3.4. Življenjski cikel gradiva, klasifikacija in uničenje

Sistem e-hrambe mora omogočati definicijo politik hrambe, ki vključujejo čas hrambe, pravila izločanja in uničenja.

Samodejno brisanje dokumentov po poteku roka hrambe mora biti:

- sledljivo v revizijski sledi,
- izvedeno šele po potrditvi pooblaščenih oseb.

Klasifikacijski načrt mora biti:

- strukturiran,
- verzioniran,
- obvezen ob zajemu dokumenta,
- tehnično povezan z metapodatkovnim modelom zapisa.

3.5. Verzije in revizijske sledi

Sistem e-hrambe mora omogočati eno- in večnivojsko verzioniranje dokumentov in metapodatkov. Starih verzij ni dovoljeno spreminjati ali brisati.



Revizijska sled mora biti nespremenljiva (immutable) in obstajati najmanj:

- na nivoju dokumenta,
- na nivoju posamezne akcije,
- na nivoju iskanja.

Revizijske sledi se hranijo najmanj toliko časa, kot velja najdaljša politika hrambe v sistemu.

3.6. Uvoz, izvoz in migracije

Sistem e-hrambe mora omogočati:

- posamični in masovni uvoz brez omejitev glede velikosti paketa,
- uvoz v strukturirani XML obliki z obvezno avtomatsko validacijo,
- zavrnitev uvoza v primeru napak z jasnim izpisom napak,
- vzporedni uvoz več paketov.

Sistem e-hrambe mora omogočati poln izvoz vseh dokumentov in metapodatkov v odprtem, dokumentiranem in strojno berljivem formatu, primernem za neposreden uvoz v drugo certificirano e-hrambo.

3.7. Integracije in API

Sistem e-hrambe mora omogočati integracije prek varnih spletnih storitev (SOAP in/ali REST). API mora omogočati uvoz, izvoz in vpogled v dokumente, dostop do metapodatkov ter revizijskih sledi

Sistem e-hrambe mora zagotavljati brezšivno integracijo z obstoječim dokumentnim sistemom naročnika (Business Connect – BC), tako da po arhiviranju dokumentov v e-hrambo uporabniki in aplikacije do dokumentov še naprej dostopajo izključno preko sistema BC. Dokument mora po prenosu ostati viden in dostopen v BC, pri čemer se vsebina dokumenta hrani v e-hrambi, BC in e-hramba pa preko brezšivne integracije zagotavljata dostop do dokumenta in pripadajočih metapodatkov, brez sprememb obstoječih poslovnih procesov, uporabniških vlog ali aplikacijskih integracij.

3.8. Uporabniški vmesnik

Uporabniški vmesnik mora biti:

- spletna HTML5 aplikacija (thin client),
- združljiv z Microsoft Edge,
- v celoti lokaliziran v slovenski jezik,
- omogočati sočasno pregledovanje in urejanje metapodatkov ter dokumentov,
- podpirati funkcionalnost povleci in spusti (Drag & Drop).

3.9. Tipi dokumentov

Za potrebe učinkovite, sledljive in dolgoročno vzdržne elektronske hrambe mora sistem e-hrambe podpirati več tipov dokumentov. Tip dokumenta predstavlja definiran metapodatkovni model za posamezno vrsto dokumentarnega gradiva. Vsak tip določa:

- nabor obveznih metapodatkov,
- nabor izbirnih metapodatkov,
- validacijska pravila,
- povezanost z veljavnim klasifikacijskim načrtom,
- posebnosti dolgoročne hrambe (format, povezane priloge).

Predvideni tipi (primer, neizčrpen seznam)

Naročnik ocenjuje, da bo potrebnih vsaj 30 ločenih tipov, odvisno od klasifikacije in strukture poslovnih procesov. Minimalni nabor vključuje:

1. Gradivo iz dokumentnega sistema BC

- tipi glede na proces ali modul znotraj BC,
- predvidenih je 10 tipov,
- različne družbe uporabljajo enak nabor metapodatkov.

2. Zajeto fizično gradivo



- obvezni metapodatki skeniranja,
- predvidenih je do 10 tipov.
- 3. Zvočno gradivo (posnetki sej)**
 - obvezni metapodatki za zvočno gradivo,
 - predviden je 1 tip.
- 4. ODOS dokumenti**
 - metapodatki iz izvoza (xlsx + priponke), pretvorjeni v XML ali drugo strukturirano obliko,
 - predvidenih je do 10 tipov.
- 5. Ostale sheme**
 - splošni metapodatkovni model za nestrukturirane dokumente.

Zahteve glede tipov dokumentov

Ponudnik mora zagotoviti:

- podporo poljubnemu številu tipov,
- možnost razširjanja tipov brez prekinjanja delovanja sistema,
- validacijo metapodatkov ob uvozu (samodejna zavrnitev neustreznih zapisov),
- enostavno prilagajanje tipov preko konfiguracije, ne razvoja,
- povezljivost tipov s klasifikacijskim načrtom naročnika,
- izvoz vseh dokumentov z metapodatkovnimi modeli v odprtem formatu.

Obvezna podpora za spremembe tipov

V času trajanja pogodbe mora ponudnik omogočati:

- dodajanje novih tipov,
- spremembe obstoječih tipov,
- upravljanje verzij tipov (verzioniranje metapodatkovnih modelov),
- migracije dokumentov med tipi (če je potrebno zaradi sprememb klasifikacije ali zakonodaje).

3.10. Iskanje dokumentov

Sistem mora zagotavljati enoten iskalni mehanizem z:

- iskanjem po vseh metapodatkih,
- full-text OCR iskanjem po vsebini dokumentov,
- podporo logičnim operatorjem AND/OR, izključitvam in nadomestnim znakom,
- omejevanjem rezultatov glede na uporabniške pravice,
- dinamično dopolnjevanje ali spreminjanje iskalnih kriterijev ter ponovno izvedbo iskanja na podlagi posodobljene iskalne definicije,
- vizualnim označevanjem iskalnih pogojev.

Iskalni indeks mora biti vključen v strategijo varnostnih kopij in obnove.

3.11. Avtentikacija in dostop

Dostop do storitev sistema e-hrambe mora ponudnik zagotoviti na dva načina:

1. Dostop do dokumentov v sistemu e-hrambe iz dokumentnega sistema BC preko brezšivne integracije (za dokumente, ki so bili preneseni v e-hrambo iz BC-ja).
2. Dostop do ostalih dokumentov v sistemu e-hrambe preko uporabniškega vmesnika e-hrambe (za dokumente, ki so bili uvoženi v e-hrambo preko masovnega uvoza (zajeti dokumenti, ODOS, ipd.) ali dodani preko uporabniškega vmesnika (npr. zvočni posnetki sej)).

Sistem e-hrambe mora omogočati:

- imenske licence, pri čemer je tip licence nastavljen na nivoju posameznega uporabnika,
- samodejno odjavo uporabnikov po času neaktivnosti,
- nastavitev maksimalnega števila neuspešnih prijav, po katerem se uporabniški račun samodejno zaklene,
- odklep uporabniškega računa izključno s strani administratorja ali na podlagi vnaprej definirane varnostne politike.

Sistem e-hrambe mora podpirati:

- centralizirano avtentikacijo prek Microsoft Entra ID ali ADFS naročnika,
- enotno prijavo (SSO),
- večfaktorsko avtentikacijo (MFA),
- vsi dogodki avtentikacije, avtorizacije in administrativna dejanja morajo biti zajeti v revizijski sledi
- avtorizacijo na podlagi skupin,
- uporabo principa najmanjših pravic (PoLP) in role-based access control (RBAC),
- podporo integraciji s centralnim Identity and Access Management (IAM) sistemom naročnika,
- privilegirani (skrbniški) dostopi morajo biti ustrezno upravljani, nadzorovani in beleženi. Sistem mora zagotavljati revizijsko sled vseh administrativnih dostopov in aktivnosti.,
- omogočena mora biti integracija z naročnikovim SIEM ali SOAR sistemom, za spremljanje in analizo administrativnih aktivnosti.

Revizijske sledi in nadzor:

- sistem mora generirati varnostne dnevniške zapise (security logs), ki omogočajo popolno revizijsko sled dogodkov,
- dnevniki morajo biti pošiljani v SIEM naročnika v standardiziranem formatu (npr. Syslog, CEF, JSON, LEEF ali drug dogovorjen format),
- minimalno zajeti dogodki morajo vključevati:
 - o prijave in odjave uporabnikov,
 - o spremembe konfiguracij in nastavitev,
 - o spremembe uporabniških ali skrbniških pravic,
 - o zaznane poskuse nepooblaščenega dostopa,
 - o aktivnosti privilegiranih uporabnikov.
- dnevniški zapisi morajo biti zaščiteni pred brisanjem in spreminjanjem (npr. WORM ali append-only shranjevanje),
- potrebno bo določiti minimalni rok hrambe logov (najmanj 6 mesecev aktivne hrambe, z možnostjo arhiviranja do 12 mesecev ali več, skladno z zahtevami naročnika),
- revizijske sledi morajo omogočati časovno usklajenost (npr. z uporabo NTP) za potrebe korelacije dogodkov v SIEM sistemu,
- naročnik in ponudnik se dogovorita o obsegu, formatu in prioriteti logiranja v fazi implementacije,
- po potrebi ponudnik in naročnik dogovorita vključitev "anomaly detection" dogodkov na podlagi logov, vključno s podatki o zaznanih odstopanjih, poskusih vdorov ali spremembah vedenja uporabnikov,
- vsi podatki o revizijskih sledih morajo biti obravnavani kot zaupni in dostopni izključno pooblaščenim osebam.

3.12. Upravljanje ranljivosti in posodobitev (Patch Management)

Sistem mora biti podprt s strani proizvajalca in redno prejemati varnostne ter funkcionalne posodobitve.

V času trajanja pogodbe mora izvajalec sistem posodobljati z zadnjimi ustreznimi varnostnimi popravki.

Za kritične ranljivosti (CVSS ≥ 9) mora izvajalec zagotoviti odpravo v največ 10 dneh od objave popravka ali potrjene ranljivosti

Za pomembne ranljivosti (CVSS ≥ 7) mora izvajalec zagotoviti odpravo v največ 30 dneh od objave popravka ali potrjene ranljivosti.

Ponudnik mora v sodelovanju z naročnikom izvajati redno posodabljanje (patching) in dokumentirati vse izvedene aktivnosti.



Pred uvedbo posodobitev v produkcijsko okolje ponudnik izvede testiranje v testnem okolju, da se preveri združljivost in stabilnost.

Ponudnik mora vse posege v produkcijsko okolje ustrezno dokumentirati in izvesti v skladu z vzpostavljenimi postopki upravljanja sprememb izvajalca.

Ponudnik mora izvajati redno spremljanje ranljivosti v vseh komponentah rešitve, vključno z uporabljenimi knjižnicami in odvisnostmi (dependency monitoring).

Ponudnik mora izvajati redne posodobitve in varnostne popravke v dogovorjenih intervalih ali na zahtevo naročnika ob zaznavi kritičnih ranljivosti.

Ponudnik mora zagotoviti, da so posodobitve uradno podpisane in preverjene s strani proizvajalca oziroma zanesljivega vira.

Ponudnik je odgovoren za zagotavljanje patch managementa za vse komponente rešitve (operacijski sistemi, aplikacije, baze, knjižnice, vmesne komponente).

3.13. Upravljanje sprememb (Change Management)

Upravljanje sprememb se mora izvajati v skladu z vzpostavljenimi postopki ponudnika, opredeljenimi v notranjih pravilih zajema in hrambe ponudnika, ki so potrjena pri Arhivu Republike Slovenije.

Vse spremembe morajo biti dokumentirane in sledljive (opis, čas izvedbe, odgovorna oseba) ter izvedene na način, ki ne ogroža zaupnosti, integritete in razpoložljivosti sistema.

Ponudnik mora naročnika predhodno obvestiti o spremembah, ki lahko vplivajo na delovanje ali varnost sistema.

3.14. Obravnava varnostnih incidentov

Ponudnik mora imeti vzpostavljen, dokumentiran in preizkušen proces za odzivanje na varnostne incidente (Incident Response Process).

V primeru, da pride do varnostnega incidenta v okolju ponudnika (npr. napad, izpad, nepooblaščen dostop, okužba z zlonamerno kodo ipd.), mora ponudnik nemudoma obvestiti naročnika, kadar:

- obstaja možnost, da incident vpliva ali bi lahko vplival na podatke, sisteme ali storitve naročnika, ali
- incident zadeva infrastrukturo, preko katere ponudnik nudi storitev naročniku.

Obvestilo mora vsebovati najmanj:

- opis dogodka in čas zaznave,
- potencialni ali dejanski vpliv,
- začasne in trajne ukrepe za obvladovanje incidenta,
- oceno časovnega okvira za obnovitev normalnega delovanja.

Naročnik incidente deli na:

- kritične incidente – kibernetiski vdor na strani ponudnika, nedelovanje sistema zaradi kibernetkega napada ali zlonamerne kode, nepooblaščen dostop, sum razkritja/odtekanja podatkov;
- nekritične incidente – izguba dostopa, nedelovanje sistema zaradi napake pri ponudniku, izpad infrastrukture, preko katere ponudnik nudi storitve naročniku (kadar vzrok ni zunanji).

Ponudnik mora zagotoviti odzivnost glede na s strani naročnika opredeljeno klasifikacijo incidentov (kritični, nekritični) ter časovnimi roki za odziv, ki so:

- za kritični incident:
 - o prvi odziv – nemudoma oziroma v največ 4 urah,

Pripombe dodal [SR2]: Ali bi bilo smiselno to točko prestaviti pod zadnje poglavje - najem 60 mesecev in tehnična podpora?

Pripombe dodal [SR3R2]: Da

Pripombe dodal [SR4]: Kotnik

Pripombe dodal [SR5]: Opredeliti kaj je vsaka kategorija

Pripombe dodal [SR6R5]: Igor Kotnik: kategorije + odzivne čase

Pripombe dodal [SR7R5]: Tomaž prilagoditi

Pripombe dodal [TŽ8R5]: Odzivni časi za kritični incident so OK, za ostale kategorije ne vem, naj Igor pove. Zaradi mene so lahko samo dve: Kritični in nekritični



- analiza in ukrepi – v največ 8 urah,
 - začetno poročilo – v največ 24 urah,
 - končno poročilo – v največ 3 delovnih dneh po odpravi posledic.
- za nekritični incident:
 - prvi odziv – nemudoma oziroma v največ 4 urah,
 - analiza in ukrepi – v največ 24 urah,
 - začetno poročilo – v 5 delovnih dneh,
 - končno poročilo – v 10 delovnih dneh.

Ponudnik mora hraniti vse relevantne dokaze in loge o incidentu ter jih na zahtevo posredovati naročniku ali pristojnim organom.

V primeru, da incident vključuje podatke naročnika (npr. osebne ali poslovno občutljive informacije), mora ponudnik zagotoviti takojšnje obveščanje in ukrepanje v skladu z zakonodajo ter internimi postopki naročnika.

3.15. Življenjski cikel in podpora

Sistem mora biti v fazi glavne (mainstream) ali razširjene (extended) podpore proizvajalca.

Uporaba nepodprtih sistemov (EoL/EoS) je prepovedana, razen če je to izjemoma pisno odobreno s strani naročnikove službe za informacijsko varnost.

Ponudnik mora zagotoviti nadgradnjo ali prilagoditev programske opreme na novejši, podprt operacijski sistem v primeru, da obstoječa platforma (npr. operacijski sistem) doseže konec življenjskega cikla ali izgubi podporo proizvajalca. Namen zahteve je zagotoviti neprekinjeno delovanje, varnostno skladnost in preprečiti uporabo nepodprtih sistemov.

V primeru, da proizvajalec programske opreme ali sistema preneha z razvojem ali zagotavljanjem podpore, mora ponudnik zagotoviti, da se ohranijo dostopnost, integriteta in uporabnost dokumentarnega gradiva ter omogočiti njegov izvoz oziroma prenos v drug ustrezen informacijski sistem za dolgoročno hrambo, skladno z ZVDAGA in Enotnimi tehnološkimi zahtevami (ETZ).

V primeru, da ponudnik preneha poslovati ali postane poslovno oziroma operativno nesposoben zagotavljati podporo, mora zagotoviti, da naročnik prejme vse potrebne informacije, tehnično dokumentacijo, konfiguracijske nastavitve, licence ter druge vire, ki omogočajo nemoteno delovanje, vzdrževanje ali prenos rešitve k drugemu izvajalcu. Namen zahteve je zagotoviti neodvisnost naročnika od posameznega ponudnika ter kontinuiteto delovanja kritičnih sistemov.

Po potrebi mora ponudnik periodično izvajati ocenjevanje arhitekture z namenom prepoznavanja in izločanja zastarelih komponent ali programske opreme, ki bi lahko ogrozile varnost ali stabilnost sistema.

3.16. Razpoložljivost in nadzor

Sistem mora biti dostopen 24/7/365.

Zahtevana razpoložljivost:

- ≥ 99,7 % za neplanirane izpade,
- ≥ 99 % za planirane izpade.

Planirani posegi morajo biti napovedani najmanj sedem (7) dni vnaprej in izvedeni izključno med 18.00 in 6.00.

3.17. Fizična in organizacijska varnost

Ponudnik mora zagotoviti, da se strežniška infrastruktura nahaja v varovanem podatkovnem centru, ki vključuje:



- nadzorovan fizični dostop (kontrola pristopa, evidence vstopov),
- video nadzor,
- redundantno napajanje in hlajenje,
- ustrezno protipožarno zaščito.

Ponudnik bo na morebitno zahtevo naročnika za vse zaposlene, ki imajo ali lahko pridobijo dostop do sistemov ali podatkov naročnika, predložil ustrezna potrdila o nekaznovanosti in zagotovil, da bodo zaposleni pristopili k podpisu pogodbe o zaupnosti (NDA).

Ponudnik mora:

- izvajati redno usposabljanje in ozaveščanje zaposlenih o varnostnih tveganjih, vključno z letnimi izobraževanji in po potrebi simulacijami phishing napadov,
- zagotoviti, da so obiski in fizični dostopi do prostorov, kjer se obdelujejo podatki naročnika, beleženi, nadzorovani in odobreni,
- imeti izdelan načrt fizične varnosti in postopke v sili (evakuacija, požar, izpad napajanja, poplava ipd.),
- vse storitve izvajati na način, ki v celoti onemogoča dostop nepooblaščenih oseb do gradiva v vseh fazah: prevzem, pretvorba, uvoz, hramba in dostop.

3.18. Usposabljanje naročnikovih uporabnikov za uporabo sistema

Ponudnik mora v enem (1) mesecu po izvedeni vzpostavitvi sistema e-hrambe izvesti usposabljanje naročnikovih uporabnikov za uporabo sistema. Usposabljanje se izvede preko testnega okolja.

3.19. Podrobnejši časovni načrt

Naročnik in izbrani ponudnik bosta podrobnejši časovni načrt izvajanja storitve vzpostavitve sistema e-hrambe dogovorila najkasneje v enem (1) mesecu od podpisa pogodbe.

4. PODPORA PRI VZPOSTAVITVI BREZŠIVNE INTEGRACIJE DOKUMENTNEGA SISTEMA BUSINESSCONNECT Z E-HRAMBO

Naročnik bo v sodelovanju z zunanjim izvajalcem izvedel integracijo dokumentnega sistema BusinessConnect z vzpostavljenim sistemom e-hrambe, pri čemer mora izbrani ponudnik zagotoviti sodelovanje in tehnično podporo.

5. PRETVORBA IN ENKRATNI UVOZ GRADIVA IZ RAZLIČNIH DATOTEK

Izbrani ponudnik mora po izvedeni vzpostavitvi sistema e-hrambe izvesti uvoz in v nekaterih primerih tudi pretvorbo naročnikovega gradiva v obsegu in na način kot izhaja iz nadaljevanja.

5.1. Obseg in struktura dokumentarnega gradiva naročnika

5.1.1. Viri dokumentacije

- dokumentni sistem BusinessConnect (BC),
- dokumentni sistem ODOS,
- zvočno gradivo (datoteke mp3),
- zajeto fizično gradivo (zajem izveden s strani zunanjega izvajalca).

5.1.2. Formati datotek

- poslovni dokumenti (pdf, pdf/a, docx, xls in ostalo),
- skenirani dokumenti (pdf/a + xml ali csv (po dogovoru)),
- zvočno gradivo (mp3),
- ostalo.



5.1.3. Oblika in pretvorba dokumentacije

Naročnik bo zagotovil, da bodo vsi dokumenti, ki bodo preko integracije preneseni iz sistema **BC** v e-hrambo, v obliki, primerni za dolgoročno hrambo. Enako velja za dokumente zajete iz **fizičnega gradiva**. Pretvorba s strani ponudnika e-hrambe v teh primerih ne bo potrebna.

Dokumente, izvožene iz sistema **ODOS**, mora izbrani ponudnik tekom samega prenosa v e-hrambo pretvoriti v format primeren za dolgoročno hrambo in izvesti optično prepoznavanje znakov (OCR). Naročnik bo pripravil izvoz metapodatkov v xlsx s povezavami do priponk.

Zvočno gradivo je v obliki MPEG-1 Layer III, 186 kb/s. Ponujeni sistem za e-hrambo ga mora ob uvozu v e-hrambo samodejno pretvoriti v zapis, ki je po mnenju Arhiva RS sprejemljiv za dolgoročno hrambo: MPEG-2 Audio Layer III (ISO/IEC 13818-3 (MP3)), pri čemer se v hrambo prenese tako originalno gradivo kot pretvorjeno.

6. OČENJENE KOLIČINE GRADIVA IN LETNI PRIRAST

V spodnji tabeli so navedene ocenjene količine gradiva po družbah glede na različne vire in predviden letni prirast. Naročnik izrecno izpostavlja, da so v nadaljevanju dokumenta navedeni obsegi dokumentacije zgolj ocenjeni in lahko (bistveno) odstopajo navzgor ali navzdol. Ponudnik se izrecno in nepogojno odpoveduje vsem zahtevkom proti naročniku zaradi nedoseganja ali preseganja ocenjenih storitev/količin. Predviden obseg naročenih storitev lahko odstopa tudi zaradi sprememb okoliščin, ki jih naročnik ne more predvideti.

Družba	Ocenjena količina gradiva v BC (GB)	Predviden letni prirast (GB)
DEM d.o.o.	265	40
HSE d.o.o.	410	50
HSE INVEST d. o. o.	50	10
RGP d. o. o.	120	30
SENG d.o.o.	380	50

Tabela 1: Ocenjene količine gradiva v BC

Družba	Ocenjena količina - ODOS (GB)	Ocenjena količina - zajeto gradivo (GB)	Ocenjena količina - zvočno gradivo (GB)	Zvočno gradivo - predviden letni prirast (GB)
DEM d.o.o.	110		40	8
HSE d.o.o.	270	100	175	15
RGP d.o.o.	30			

Tabela 2: Ocenjene količine ostalega gradiva

7. ELEKTRONSKA HRAMBA DOKUMENTACIJE S TEHNIČNO PODPORO

Najem storitve e-hrambe, integracijskih in uporabniških licenc teče od dneva vzpostavitve sistema e-hrambe in se izvaja v obdobju šestdeset (60) mesecev.

Prevzeto dokumentacijo bo izvajalec elektronsko hranil od njenega uvoza v elektronsko hrambo do izteka obdobja najema storitve e-hrambe, opredeljenega v prejšnjem odstavku.

Ves čas trajanja najema e-hrambe bo ponudnik zagotavljal učinkovito tehnično podporo, s katero bo zagotovljena razpoložljivost kot v poglavju 3.16 tega dokumenta.

O pomanjkljivostih v delovanju bo izvajalca obveščal naročnik na način, dogovorjen med pogodbenima predstavnikoma naročnika in ponudnika.

7.1. Upravljanje kadrovskih sprememb pri ponudniku

Ponudnik mora imeti vzpostavljen postopek obvladovanja kadrovskih sprememb, ki zagotavlja pravočasno obveščanje naročnika o vseh spremembah, ki lahko vplivajo na dostop do podatkov naročnika.

V primeru, da obvestilo ni podano pravočasno in pride do zlorabe ali incidenta, je ponudnik v celoti odgovoren za povzročeno škodo.

Evidenca in preverjanje

Ponudnik mora voditi ažurno evidenco vseh oseb, ki imajo ali so imele dostop do sistemov ali podatkov naročnika.

Evidenca mora vključevati ime, priimek, organizacijsko enoto, vlogo, datume dodelitve in preklica dostopa. Na zahtevo naročnika mora ponudnik posredovati evidenco ali sodelovati pri pregledu dostopov (user access review).

Naročnik si pridržuje pravico do preverjanja skladnosti postopkov ponudnika glede obveščanja, dodeljevanja in preklica dostopov.

Možnost preverjanja skladnosti postopkov

Naročnik si pridržuje pravico do preverjanja skladnosti izvajanja postopkov, povezanih z obveščanjem, dodeljevanjem, spreminjanjem in preklicem uporabniških dostopov pri ponudniku.

Preverjanje se lahko izvede v obliki:

- notranje revizije naročnika,
- neodvisnega pregleda s strani tretje pooblaščen osebe, ali
- zahteve za posredovanje dokazil o izvedenih postopkih in kontrolah.

Ponudnik mora na zahtevo naročnika omogočiti vpogled v:

- evidence zaposlenih z dostopi do sistemov in podatkov naročnika,
- postopke preverjanja identitete oseb,
- evidence o dodelitvi, spremembi in ukinitvi dostopov,
- zapise o izvedenih varnostnih preverjanjih, NDA pogodbah in usposabljanjih zaposlenih.

V primeru ugotovljenih odstopanj mora ponudnik pripraviti načrt korektivnih ukrepov (Corrective Action Plan) in naročniku v določenem roku posredovati dokazila o odpravi pomanjkljivosti.