

VÄIKEHANGE „Vibecoding-rakenduste turvalise CI/CD konveieri ja isoleeritud pilvekeskkonna loomine“

Käesoleva dokumendiga kutsub Justiits- ja Digiministeerium Teid esitama pakkumust väikehankel.

HINNAPÄRING	
1. ÜLDINFO	
1.1 Hankija andmed	Justiits- ja Digiministeerium Suur-Ameerika 1, 10122 Tallinn, Eesti Vabariik
1.2 Hanke eest vastutav isik	Karmen Vilms, telefon: 502 7190, e-post: Karmen.Vilms@justdigi.ee
1.3 Hanke objekti lühikirjeldus ja eesmärk	Hanke eesmärk on leida partner, kes ehitab automaatse CI/CD konveieri, mis viib hankija koodirepositooriumist lähtekoodi turvaliselt ja korratavalt isoleeritud pilvekeskkonda. Lisaks seadistatakse eraldatud pilvekeskkond, kus vibecode-itud proof-of-concept rakendused on üksteisest sõltumatud, pääsevad välisvõrku vaid konveieri lubatud ulatuses ja on vaikumisi kättesaadavad ainult sisevõrgust. Partner annab üle ka kohustusliku vaikumisi templiidi, mis suunab mittearendajate loodud koodi ühtsete, lihtsate ja turvaliste lahenduste poole ning mille reeglid jõustatakse automaatselt.
1.4 Eeldatav maksumus km-ta ¹	29 999
1.5 Teenuse CPV kood	72200000-7
1.6 Isikuandmete töötlemine	Isikuandmete töötlemisel tuleb järgida isikuandmete kaitse seaduses ja üldmääruses (EL 2016/679) sätestatud
1.7 Riigihangete strateegiliste põhimõtete kasutamine	- Keskkonnahoidlik hankimine: ei - Sotsiaalselt vastutustundlik hankimine: ei - Innovatsiooni toetav hankimine: jah - Julgeolekuriske vähendav: ei
2. HANKE OBJEKTI TEHNILINE KIRJELDUS/ OLULISEMAD TINGIMUSED	
2.1 Hanke objekti kirjeldus	Hanke objekt. Hanke esemeks on tarkvara juurutuskonveieri ja isoleeritud pilvekeskkonna arendus- ja seadistusteenus, mille käigus partner projekteerib, ehitab, dokumenteerib ja annab tellijale üle terviklahenduse, mis võimaldab ärikasutajatel AI abil loodud (vibecode-itud) rakendusi automaatselt, turvaliselt ja korratavalt eraldiseisvasse pilvekeskkonda juurutada ning neid reaalselt kasutada. Eesmärk ja taust. Organisatsioonis luuakse rakendusi mudeli alusel, kus ärikasutaja loob kohustusliku templiidi alusel rakenduse, mida käsitletakse proof-of-concept lahendusena. Hanke eesmärk on luua tehniline platvorm ja protsess, mis suunab sellise arenduse ühtsete, lihtsate ja turvaliste lahenduste poole ning maandab AI-genereeritud koodi riske automaatse, inimese käsitsi ülevaatusest sõltumatu vastavuskontrolli kaudu. Hange hõlmab nelja omavahel seotud tarnet:

¹ eeldatav maksumus on hankija poolt hankelepingu täitmisel eeldatavalt makstav kogusumma (käibemaksuta), arvestades mh töönaolisi hankelepingu alusel tulevikus tekkivaid kohustusi ja hankelepingu uuendamist. Füüsiliste isikutega sõlmitavate lepingute korral tuleb eeldatava maksumuse sisse arvestada ka tööandja maksud ja maksed.

	1. CI/CD konveier — automaatne torustik, mis võtab hankija GitHubi lisatud lähtekoodi ja rakendab kõik vajalikud sammud (ehitamine ja pakendamine, sõltuvuste kontroll heakskiidetud paketi peegli kaudu, turva- ja kvaliteediskannerid, policy-as-code vastavuskontroll, saladuste haldus, artefaktihoidla ning keskkonnateadlik juurutus) kuni rakenduse juurutamiseni i3 keskkonda. 2. Isoleeritud i3 pilvekeskkond — Kubernetese-põhine keskkond, kus juurutatud lahendused on üksteisest sõltumatud nii turvalisuse kui jõudluse mõttes, pääsevad välisvõrku ainult konveieri poolt deklareeritud ulatuses, ei oma ligipääsu organisatsiooni sisevõrku ning on vaikimisi kättesaadavad ainult sisevõrgust (välisvõrgust ligipääs üksnes erandkorras ja erikokkuleppel). 3. Vaikimisi templiit — kohustuslik lähtekomplekt, mis koondab rakenduse loomise tehnilised nõuded, oskused ja konteksti, on masinloetavalt seotud konveieri vastavuskontrollidega ning suunab koodi lihtsuse, modulaarsuse, testituse ja jätkusuutlikkuse poole. 4. Piiratud mahus toe pakkumine hankija poolt loodud rakenduste paigaldamiseks ja majutamiseks hanke käigus loodud konveierit kasutades. Lisaks kuuluvad objekti juurde ühised nõuded (turvalisus, jälgitavus, dokumentatsioon), vastuvõtukriteeriumide täitmine, tööjuhendite (runbook'ide) tarne ning tellija meeskonna koolitamine ja teadmussiire lahenduse iseseisvaks käitamiseks ja edasiarendamiseks. Peamised tingimused. Lahendus peab olema täisautomaatne, korratav ja kirjeldatud koodina; turvalisus ja isolatsioon peavad olema vaikeseaded (secure by default, deny by default); reeglid tuleb jõustada automaatselt nii konveieris kui klatri sissepääsu juures. Dokument kirjeldab nõudeid, mitte konkreetseid tootevalikuid — tehnoloogiate valik ja põhjendus on pakkuja ülesanne ning kooskõlastatakse tellijaga enne tööde algust. Tööde täpsem kirjeldus on lisa 1 – Tehniline kirjeldus
2.2 Tähtaeg ja/või ajakava	Lepingu täitmise tähtaeg on 01.12.2026.
2.3 Lepingutingimused	- Lepingu täitmisel kohaldatakse Justiits- ja Digiministeeriumi töövõtulepingu üldtingimusi, mis on kättesaadavad Justiits- ja Digiministeeriumi kodulehel aadressil: https://www.justdigi.ee/majandusteave-ja-riigihanked#justiitsministeeriumi_lepingute_uldtingimused - Lepingu eritingimused on toodud väikehanke dokumendi lisa (lisa 2 – lepingu eritingimuste projekt).
2.4 Samaväärsus	Iga viidet, mille hankija teeb väikehanke dokumentides mõnele standardile, tehnilisele tunnustusele, tehnilisele kontrollisüsteemile vms kui pakkumuse tehnilisele kirjeldusele vastavuse kriteeriumile, tuleb lugeda selliselt, et see on täiendatud märkega „või sellega samaväärne“. Iga viidet, mille hankija teeb väikehanke dokumentides ostuallikale, protsessile, kaubamärgile, patendile, tüübile, päritolule või tootmisviisile, tuleb lugeda selliselt, et see on täiendatud märkega „või sellega samaväärne“.
2.5 Keskkonnahoidlike lahenduste kasutamine	Pakkuja peab hankelepingu täitmisel eelistama keskkonnahoidlikke lahendusi, näiteks:

	1) töökoosolekud ja muud kohtumised viia läbi võimaluse korral veebi vahendusel, et vähendada eelkõige liigsest transpordikasutusest tulenevat süsiniku jalajälge; 2) vältida tarbetut dokumentide välja trükkimist ning võimalusel eelistada digitaalsel kujul olevaid materjale; 3) pakkuja poolt digitaalsel kujul edastatavad materjalid peavad olema salvestatud ja edastatud optimaalse mahuga, et vältida otstarbetult suuri andmefailide ning seega vähendada digireostust; 4) hankelepingu täitmise järgselt kustutada üleliigsed digimaterjalid, näiteks mustandfailid, säilitamiseks mittevajalikud töödokumendid jms, kuna IT-serverites failide otstarbetu hoidmine on keskkonda kurnava mõjuga ning suurendab digireostust
2.6 Võrdse kohtlemise tagamine ja mitte-diskrimineerimine	Pakkumuse esitamisega kinnitab pakkuja, et juhindub meeskonna komplekteerimisel Euroopa Parlamendi ja nõukogu määruse (EL) nr 1303/2013 artiklist 7, mis näeb ette, et arvestatakse ja toetatakse meeste ja naiste võrdõiguslikkust ja välditakse diskrimineerimist soo, rassi või rahvuse, usutunnistuse või veendumuse, puude, vanuse või seksuaalse sättumuse põhjal ning võetakse arvesse puuetega inimeste juurdepääsu. Ühtlasi lähtutakse Eesti pikaajalise arengustrateegia „Eesti 2035“ aluspõhimõtetest, mis näeb ette, et kõigil peab olema võrdne võimalus eneseteostuseks ja ühiskonnaelus osalemiseks, sõltumata individuaalsetest eripäradest ja vajadustest, kuuluvusest erinevatesse sotsiaalsetesse rühmadesse, sotsiaal-majanduslikust võimekusest ja elukohast
3. TÄIENDAV INFO	
3.1 Pakkujale ja pakkumusele kehtestatavad nõuded	- Pakkuja peab omama varasemalt kogemust CI/CD konveierite loomisel ning tehisaru poolt loodud tarkvara paigaldamisel ning majutamisel. - Pakkuja peab töö teostamiseks komplekteerima vajaliku meeskonna sellises mahus nagu pakkuja vajalikuks peab, et töö saaks edukalt ning õigeaegselt teostatud.
4. PAKKUMUSE ESITAMINE ja MENETLEMINE	
4.1 Selgitused	- Huvitatud isikutel on õigus küsida väikehanke dokumentide kohta selgitusi, esitades küsimused e-posti aadressile: evan.somer@justdigi.ee ja karmen.vilms@justdigi.ee. Hankija vastab huvitatud isiku küsimustele 3 tööpäeva jooksul. Hankija edastab esitatud küsimused ja vastused samaaegselt kõigile isikutele, kellele tehti ettepanek pakkumuse esitamiseks.
4.2 Pakkumuse vormistamine ja esitamine	- o Pakkumuses esitab pakkuja: - o Pakkumuse vormi koos kinnitustega (lisatud pakkumuskutsele); - Teostatava töö lühikirjeldus lähtudes Lisast 1; - Vajaduste (tehniliste, inimressursi jne) nimekiri, mida Pakkujal on Hankijalt vaja lepingu edukaks täitmiseks; - Planeeritud meeskonnaliikmete nimekiri koos CV-dega; - o Pakkuja kannab kõik pakkumuse ettevalmistamise ja esitamisega seotud kulud ning pakkumuse tähtaegse esitamise riski. - o Esitatud pakkumus peab olema jõus vähemalt 60 päeva alates pakkumuste esitamise tähtpäevast. - o Pakkumus tuleb esitada digitaalselt allkirjastatult e-posti aadressil info@justdigi.ee hiljemalt 7.08.2026 kell 12:00.

	○ Palume ühtlasi, et teavitaksite meid, kui otsustate pakkumust mitte esitada. ○ Pakkumus on konfidentsiaalne kuni hankelepingu sõlmimiseni. ○ Pakkuja märgib pakkumuses, milline teave on pakkuja ärisaladus ning põhjendab teabe ärisaladuseks määramist. Pakkuja ei või ärisaladusena märkida pakkumuse maksumust või osamaksumusi. Hankija ei avalikusta pakkumuste sisu ärisaladusega kaetud osas. Hankija ei vastuta ärisaladuse avaldamise eest osas, milles pakkuja ei ole seda ärisaladuseks märkinud.
4.3 Pakkumuse vastavuse kontrollimine	- Hankija avab kõik tähtjaks esitatud esialgsed pakkumused ning kontrollib esitatud pakkumuste vastavust väikehanke dokumendis sätestatud nõuetele. - Juhul kui pakkuja või pakkumus ei vasta väikehanke dokumendis esitatud tingimustele, siis lükkab hankija pakkumuse tagasi. - Hankijal on õigus tagasi lükata pakkumus, mille maksumus nõuaks riigihangete seaduse kohaselt toiminguid riigihangete registris.
4.4 Pakkujaga läbirääkimiste pidamine	- Hankija võib pidada kõikide vastavaks tunnistatud pakkumuse esitanud pakkujatega läbirääkimisi esitatud pakkumuse sisu, ajakava ja maksumuse üle. Läbi ei räägita väikehanke dokumendi pakkuja ja pakkumusele sätestatud nõuete ja hindamiskriteeriumide üle. - Läbirääkimiste ajal tagab hankija kõigi pakkujate võrdse kohtlemise ega avalda läbirääkimiste käigus saadud teavet diskrimineerival viisil, mis võiks anda ühele pakkuja eelise teiste pakkujate ees. Hankija ei avalda pakkuja esitatud konfidentsiaalset teavet teistele läbirääkimistes osalejatele ilma pakkuja nõusolekuta. - Läbirääkimisi võib pidada vastavalt hankija ja pakkujate kokkuleppele, kas elektrooniliselt või koosoleku vormis. Suuliselt peetud läbirääkimised protokollitakse. - Läbirääkimiste lõppedes võib hankija teha pakkujatele ettepaneku lõplike, kohandatud pakkumuste esitamiseks.
4.5 Pakkumuste hindamine	- Hankija hindab kõiki vastavaks tunnistatud pakkumusi. Hankijal on õigus vajadusel pakkumusi omavahel võrrelda. - Edukaks tunnistatakse majanduslikult soodsaim so madalaima kogumaksumusega pakkumus.
4.6 Pakkuja teavitamine hankija otsustest ja lepingu sõlmimine	- Hankija esitab kõigile pakkujatele teate hankelepingu sõlmimise kohta mitte hiljem kui 3 tööpäeva jooksul alates lepingu sõlmimisest. - Hankija sõlmib edukaks tunnistatud pakkumuse esitanud pakkujaga lepingu.

Pakkumuse vorm 5-6/5540

Pakkuja üldandmed

Pakkuja ärinimi	
Pakkuja registrikood	
Pakkuja juriidiline aadress	
Pakkuja esindaja lepingu allkirjastamisel	
Pakkuja kontaktisik/ volitatud isik lepingu täitmisel - nimi ning kontaktandmed (e-posti aadress, telefoninumber)	

Pakkumuse maksumus *kuluartiklite* lõikes

Kuluartikkel	Ühik	Ühiku hind	Ühiku arv	KOKKU (eurot)
Pakkumuse maksumus (ilma käibemaksuta)				
Käibemaks:				
Pakkumuse kogumaksumus (käibemaksuga)				

1. Kinnitame, et pakutav hind sisaldab kõiki tasusid ning pakkuja on teadlik, et tal ei ole õigust täiendavale tasule pakkumuse lähteülesande alusel tehtava töö eest.
2. Kinnitame, et pakkumus on jõus vähemalt väikehanke dokumendis märgitud tähtaja.
3. Kinnitame, et pakkuja on teadlik, et hankija ei kasuta arveldamises ettemaksu.
4. Kinnitame, et kasutame lepingu täitmisel keskkonnahoidlikke lahendusi.
5. Kinnitame, et oleme meeskonna komplekteerimisel järginud võrdse kohtlemise ja mitte-diskrimineerimise põhimõtteid.
6. Kinnitame, et pakkuja on teadlik, et tal tuleb märkida pakkumuses, milline teave on pakkuja ärisaladus ja põhjendada seda ning selle nõude mittetäitmisel kannab pakkuja riisikot, et hankija avalikustab pakkumuse sisu, mida ei ole ärisaladuseks märgitud.

Lisa 1 - Tehniline kirjeldus

CI/CD konveier ja isoleeritud i3 pilvekeskkond vibecoditud rakenduste majutamiseks ja kasutamiseks

1. Sissejuhatus ja eesmärk

Hanke eesmärk on leida partner, kes projekteerib ja ehitab valmis kaks omavahel seotud komponenti:

A. Automaatse CI/CD **konveieri (pipeline)**, mis võtab hankija GitHubi lisatud lähtekoodi ja rakendab kõik vajalikud sammud, et koodi turvaliselt ja korratavalt Kubernetese-põhisesse pilve deployda.

B. Eraldiseisva **pilvelahenduse platvormil nimega i3**, kuhu neid rakendusi deployda. Platvorm peab tagama, et sinna deploytud lahendused on üksteisest sõltumatud (nii turvalisuse kui jõudluse mõttes), pääsevad välisvõrku ainult siis, kui konveier on selle otsesõnu lubanud, ning on vaikimisi kättesaadavad ainult sisevõrgust.

Komponendid moodustavad ühtse platvormi, mille kaudu äripool saab templiidi alusel loodud rakendusi turvalisse, isoleeritud keskkonda deployda ja reaalselt kasutada.

Lisaks nimetatud komponentidele peab pakkuja tellijale üle andma **vaikimisi templiidi** (vt ptk 7), mida rakendatakse iga arenduse puhul, mida pakkuja loodud konveier suudab deployda.

Käesolev dokument kirjeldab **nõudeid**, mida lahenduse loomisel tuleb järgida. Dokument ei kirjuta ette konkreetseid tehnoloogiaid ega tootevalikuid — nende valik ja põhjendus on pakkuja ülesanne, kui käesolevas dokumendis pole otsesõnu teisiti nõutud. Kus tooteid on nimetatud, on need üksnes olemasoleva keskkonna kirjeldus või mittesiduv näide (märgitud sõnaga „nt”).

2. Taust ja kontekst

Organisatsioonis luuakse rakendusi „vibecoding” mudeli alusel: ärikasutaja loob rakenduse, lähtudes kohustuslikust **templiidist** (mis ühendab rakenduse loomise tehnilised nõuded, oskused ja konteksti — vt ptk 7). Sellised rakendused on käsitletavad **proof-of-concept (PoC)** lahendustena — äri võib neid tööks kasutada ning töö käigus edasi täiendada lähtuvalt praktikas selguvatest vajadustest. Kui PoC osutub väärtuslikuks, antakse see arendustiimile üle ja käsitletakse edaspidi tavapärase tarnena.

Hangitav konveier ja i3 pilve majutus teenindavad selle mudeli **PoC-etappi**: nad peavad võimaldama sellise koodi automaatset, turvalist ja isoleeritud deploymist, ilma et see saaks mõjutada teisi lahendusi või organisatsiooni sisevõrku.

Kuna märkimisväärne osa koodist on genereeritud AI abil, tuleb erilist tähelepanu pöörata tarneahela turvalisusele (sh sõltuvuste päritolu ja usaldusväärsus) ning automaatsele vastavuskontrollile — inimese käsitsi ülevaatusele ei tohi lahendus tugineda ning inimese sekkumine paigaldusprotsessi peab olema minimaalne.

3. Hanke ese ja ulatus

Hanke esemeks on järgmiste tarnete projekteerimine, ehitamine, dokumenteerimine ja üleandmine:

1. **Osa A** — GitHubi lähtekoodist i3 pilve deployv CI/CD konveier koos kõigi turva-, vastavus- ja kvaliteedisammudega (ptk 5).
 2. **Osa B** — i3 pilvekeskkond koos isolatsiooni-, võrgu- ja ligipääsumehhanismidega (ptk 6).
 3. **Osa C** — vaikimisi templiit, mis on kaasas iga deploytava arendusega (ptk 7).
 4. **Ühised nõuded** — turvalisus, jälgitavus, dokumentatsioon ja teadmussiire (ptk 8).
 5. **Üleandmine ja teadmussiire** — vastuvõtukriteeriumide täitmine ja meeskonna koolitamine (ptk 9–10).
 6. **40h ulatuses konsultatsiooni** – tellija toetamiseks Osa A – C-ga seotu praktilisel kasutamisel
-

4. Mõisted

Mõiste	Selgitus
Konveier / pipeline	Automaatne CI/CD protsess, mis viib lähtekoodi valmis, deploytud rakenduseni.
i3	Käesoleva hankega loodav eraldiseisev pilveplatvorm PoC-lahenduste majutamiseks.
Töökoormus (workload)	Üks deploytud rakendus või selle komponent i3 keskkonnas.
Isolatsioon	Töökoormuste eraldatus võrgu, arvutusressursi ja andmete tasemel nii, et üks ei saa teist mõjutada.
Egress	Töökoormuse väljuv võrguühendus välisvõrku / internetti.
Ingress	Sissetulev ühendus töökoormuseni (rakenduse serveerimine kasutajale).
Policy-as-code	Reeglid masinloetaval kujul, mida jõustatakse automaatselt (konveieris ja/või klastris).
Vastavuskontroll (guardrail)	Automaatne kontroll, mis takistab reeglitele mittevastava tarne edasiliikumist.
Templiit	Vaikimisi lähtekomplekt (mall), mis koondab rakenduse loomise tehnilised nõuded, oskused ja konteksti. Ühendab käesolevas

dokumendis varem eraldi kasutatud mõisted „templiit” ja „tehnilised reeglid”.

5. Osa A — Nõuded CI/CD konveierile

5.1 Üldnõuded

- **A1.** Konveier peab olema täisautomaatne: lähtekoodi muudatusest kuni i3 keskkonda deployamiseni ei tohi olla vaja käsitsi vahesamme, välja arvatud selgelt määratletud heakskiidupunktid (kui neid nõutakse).
- **A2.** Konveier peab olema **korratav ja deterministlik** — sama sisend annab sama tulemuse, sõltumata sellest, kes või millal seda käivitab.
- **A3.** Konveieri konfiguratsioon peab olema versioonihalduses (pipeline-as-code) ja auditeeritav.
- **A4.** Konveier peab olema **taaskasutatav mustrina** uute rakenduste jaoks nii, et uue rakenduse lisamine ei nõuaks konveieri nullist ülesehitamist (nt jagatud/parameetriseeritav mall).
- **A5.** Iga konveieri käivitus peab jätma tervikliku, muutmatu **auditjälje**: kes käivitas, mis koodiversioon, millised sammud läbiti, mis tulemustega ja mida deployiti.
- **A6.** Konveier ei tohi eeldada inimese käsitsi tehtud turvaülevaatust — kõik kohustuslikud kontrollid peavad olema automaatsed ja blokeerivad.

5.2 Lähtekoodi käsitus

- **A7.** Sisendiks on hankija GitHubi hoidlasse lisatud lähtekood; konveier peab käivituma määratletud sündmustest (nt muudatuse lisamine, märgistamine).
- **A8.** Konveier peab kontrollima lähtekoodi terviklikkust ja päritolu (nt commit’ide autentsus/allkirjastatus, kaitstud harud) ulatuses, mille pakkuja tellijaga kokku lepib.
- **A9.** Ligipääs lähtekoodile ja konveieri õigustele peab järgima vähima õiguse põhimõtet.

5.3 Sõltuvuste haldus ja tarneahela turvalisus

- **A10.** Konveier peab tõmbama tarkvarasõltuvused **ainult kontrollitud, sisemisest allikast** (nt privaatne paketipeer/proxy), mitte otse avalikest registritest.
- **A11.** Lubatud on ainult **heakskiidetud ja skannitud** sõltuvused; tundmatu või lubatud-nimekirjas puuduv sõltuvus peab konveieri **peatama**. See nõue maandab AI-genereeritud koodi riski viidata olematutele või pahatahtlikele pakettidele.
- **A12.** Iga tarne kohta peab tekkima **koostisosade nimekiri** (tarkvara komponendid ja nende versioonid), mis on hiljem auditeeritav.
- **A13.** Ehitatud artefaktid (nt konteineritõmmised) peavad olema **terviklikkuse mõttes tõestatatavad** (nt allkirjastatud), ja i3 keskkonda tohib jõuda ainult sellisel viisil kinnitatud artefakt (vt B-osa admission-nõuded).

5.4 Ehitamine ja pakendamine

- **A13a.** Konveier peab rakenduse **ehitama ja pakendama** deployitavaks artefaktiks (nt konteineritõmmiseks) korrataval ja deterministlikul viisil (kooskõlas A2). Ehitamine peab

kasutama ainult kontrollitud allikast tõmmatud sõltuvusi (vt A10–A11) ja heakskiidetud baastõmmiseid/-keskkondi.

- **A13b.** Ehitatud artefakt peab olema **versioonitud ja jälgitavalt seotud** lähtekoodi versiooniga (nt commit/tag), et A12–A13 nõuded (koostisosade nimekiri, terviklikkuse tõestatavus) oleksid täidetud ning downstream-sammud (skannimine, deploy, i3 admission) saaksid tarbida just seda artefakti, mille konveier ehitas.
- **A13c.** Ehitatud artefaktid (nt konteineritõmmised) peavad enne deploymist ja i3 admission-kontrolli olema hoitud selleks ettenähtud **usaldusväärses sisemises artefaktihoidlas (image registry)**. Deploy ja i3 admission tohivad artefakte tõmmata **ainult sellest registrist**; registriväliste või otse avalikest allikatest pärit tõmmiste kasutamine peab olema keelatud (kooskõlas A13 ja B21). Sissetulevate sõltuvuste paketi peegel (A10) ja väljundartefaktide registri roll on eraldiseisvad ja mõlemad peavad olema katetud.

5.5 Kvaliteedi- ja turvakontrollid

- **A14.** Konveier peab sisaldama vähemalt järgmisi automaatseid ja **blokeerivaid** kontrole:
 - saladuste tuvastus (secret detection) lähtekoodis;
 - staatiline koodianalüüs (koodi kvaliteet ja turvavead);
 - sõltuvuste haavatavuse analüüs;
 - konteineri-/artefaktiturbe skann;
 - litsentsivastavuse kontroll;
 - automaatne AI-põhine koodiülevaatus.
- **A15.** Iga kontrolli tulemuse **läviväärtused** (mis tase peatab tarne) peavad olema konfigureeritavad ja versioonihalduses.
- **A16.** Konveier peab käivitama rakenduse **automaattestid** ja peatama tarne testide ebaõnnestumisel.
- **A17.** Kontrollide tagasiside peab olema selge ja tegevusele suunatud, arusaadav ka mittearendajast kasutajale (võimalusel viidatuna konkreetsele probleemikohale ja lahendussuunale).

5.6 Reeglite jõustamine (policy-as-code)

- **A18.** Templiidis kirjeldatud nõuded (vt ptk 7 — nt logimine, struktuur, modulaarsus, nimetamine, ressursipiirangud) peavad olema jõustatud **masinloetavate poliitikatena**, mitte üksnes dokumendina.
- **A19.** Reeglitele mittevastav tarne peab konveieris **kukkuma** ega tohi jõuda i3 keskkonda.
- **A20.** Sama reeglistik peab olema jõustatud **järjepidevalt** nii konveieris kui ka i3 klatri sissepääsu juures (vt B-osa), nii et konveierist möödaminnes ei saa reegleid rikkuda.

5.7 Saladuste haldus

- **A21.** Konveier ei tohi hoida ega logida saladusi (paroolid, võtmed, credentialid) avatekstina; saladused peavad tulema selleks ette nähtud saladuste halduse teenusest.
- **A22.** Konveier peab toetama saladuste **automaatset edastamist** deploytavale töökoormusele ilma neid koodi või artefakti kirjutamata.

- **A23.** Kasutatavad volitused peavad olema **lühiajalised** ja võimalikult vähese ulatusega; pikaajaliste staatiliste saladuste kasutamist tuleb vältida.

5.8 Deploy i3 keskkonda

- **A24.** Konveier peab deployma rakenduse **ainult i3 keskkonda** ja ainult selleks ettenähtud, isoleeritud sihtkohta.
- **A25.** Deploy peab olema **keskkonnateadlik** — sihtkoht, keskkonna parameetrid ja konfiguratsioon peavad tulema versioonihalduses olevast, deklaratiivsest allikast.
- **A25a.** Pakkuja peab tarnima **keskselt hallatava, jagatud deploy-teegei/mustri** (nt ühtne Helm library vms), mida iga rakendus tarbib ja mis määrab standarditult keskkonna, sihtkoha ja deploy-reeglid. Teek peab olema versioonihalduses ja **keskselt uuendatav** nii, et muudatus ühes kohas levib kõigile rakendustele, ilma et seda tuleks igas repos eraldi dubleerida.
- **A25b.** Jagatud deploy-teegei puhul peab olema määratud **halduse (management) vastutus** — teegei elutsüklil, versioonimine, uuendamine ja aegunud versioonide käsitlemine (kooskõlas C8 laiendatavuse ja C5 standardimise nõuetega).
- **A26.** Konveier peab **deklareerima iga rakenduse võrgunõuded** (sh vajalikud väljuvad ühendused). i3 keskkond tohib lubada egress-ühendusi ainult konveieri poolt deklareeritud ulatuses (vt B-osa). Nõuded, kuidas konveierile antakse edasi võrgunõuete deklaratsioon, peab tulenema templiidist (Osa - C).
- **A27.** Konveier peab **deklareerima rakenduse kättesaadavuse ulatuse** (vaikimisi ainult sisevõrk; erandkorras välisvõrk — vt B16–B20).
- **A28.** Konveier peab tagama **turvalise tagasipööramise (rollback)** eelmisele töötavale versioonile, kui deploy ebaõnnestub.
- **A29.** Deploy peab olema idempotentne ja korduval käivitamisel ohutu.

5.9 Jälgitavus ja logimine

- **A30.** Konveier peab tagama, et iga deploytud rakendus vastab **logimise miinimumnõuetele** (määratletakse tellijaga) ja et logid suunatakse tsentraalsesse kogumisse.
- **A31.** Konveieri enda sammud, tulemused ja otsused peavad olema logitud ja jälgitavad.

5.10 Kasutuslihtsus

- **A32.** Uue rakenduse konveierisse lisamine peab olema **võimalikult lihtne** ja standarditud (eesmärk: minimaalne käsitsi seadistus, „turvaline tee on ühtlasi lihtsaim tee“).
- **A33.** Vearaportid ja tarne staatus peavad olema kasutajale nähtavad ühes kohas.

6. Osa B — Nõuded i3 pilvekeskkonnale

6.1 Sissejuhatus

i3 on RIT-i poolt pakutav PaaS teenus, mille eesmärk on pakkuda avaliku sektori infosüsteemidele standardiseeritud, kõrgkäideldavat ja hukukindlat platvormi. i3 pakub hallatud Kubernetes platvormi rakenduste jooksupäramiseks, platvormi sisse ehitatud teenuseid (nt

PostgreSQL, RabbitMQ, Redis jms), turvalisuse, monitooringu, varunduse ja paikamise teenuseid platvormi osana.

6.2 Töökoormuste isolatsioon ja sõltumatus

- **B1.** Keskkond peab olema **provisioneeritav ja taasloodav automaatselt** ilma käsitsi seadistusega.
- **B5.** Igale deployitud lahendusel peab olema oma **loogiliselt eraldatud ala** (nt eraldi nimeruum/tenant), nii et üks lahendus ei näe ega saa muuta teise ressursse.
- **B6.** Töökoormused peavad olema **võrgu tasemel üksteisest eraldatud** — vaikinisi ei tohi üks töökoormus teisega suhelda, kui seda pole otsesõnu lubatud (vaikekeeld, „deny by default“).
- **B7.** Töökoormused peavad olema **ressursside (jõudluse) mõttes eraldatud**: ühe rakenduse ressursikasutus (protsessor, mälu, salvestus, võrk) ei tohi kahjustada teiste käideldavust ega jõudlust.
- **B8.** Igale töökoormusele peavad kehtima **ressursipiirangud ja -kvoodid**, et vältida ressursside ammendamist (sh „noisy neighbor“ olukorrad).
- **B9.** Isolatsioon peab kehtima ka **andmete tasemel** — ühe lahenduse andmetele (sh salvestus ja saladused) ei tohi teine lahendus ligi pääseda.
- **B10.** Ühe töökoormuse kompromiteerimine ei tohi anda ligipääsu teistele töökoormustele ega platvormi juhtimistasandile (blast radius’e piiramine).

6.3 Väljuv võrgupääs (egress)

- **B11.** Vaikinisi peab töökoormustel olema **väljuv ühendus keelatud**.
- **B12.** Egress välisvõrku/interneti tohib olla lubatud **ainult ulatuses, mille konveier on rakenduse jaoks deklareerinud** (vt A26).
- **B13.** Lubatud egress peab olema piiratud sihtkoha täpsusega (nt lubatud sihtkohtade nimekiri), mitte üksnes „kõik või mitte midagi“.
- **B14.** Töökoormustel ei tohi olla ühtki teed organisatsiooni **sisevõrku** — i3-st sissepoole suunatud ühendus peab olema võimatu.
- **B15.** Egress-reeglite muutmine peab käima sama kontrollitud, deklaratiivse protsessi kaudu (mitte käsitsi klastris).

6.4 Rakenduste kättesaadavus (ingress)

- **B16.** i3-s serveeritavad rakendused peavad olema **vaikinisi kättesaadavad ainult sisevõrgust**.
- **B17.** Platvorm peab võimaldama **erandkorras ja erikokkuleppel** deployda rakenduse nii, et see on kasutatav ka **välisvõrgust**.
- **B18.** Väline kättesaadavus peab olema **selgesõnaline, jälgitav ja heakskiidetud otsus** (mitte vaikeväärtus), deklareeritud konveieri kaudu (vt A27) ja eraldi kinnitatav.
- **B19.** Väliselt avatud rakenduste puhul peavad kehtima **rangemad kaitsemeetmed** (nt liikluse krüpteerimine, autentimine/juurdepääsu kontroll, väärkasutuse piiramine), mille ulatus lepitakse tellijaga kokku.

- **B20.** Ingressi seadistus (sise/välis) peab olema **auditeeritav** ja igal ajahetkel peab olema võimalik välja selgitada, millised rakendused on välisvõrgust ligipääsetavad.

6.5 Klastri sissepääsu kontroll (admission)

- **B21.** i3 peab jõustama **sissepääsu-poliitika** nii, et klastrisse pääseb ainult reeglitele vastav töökoormus (nt lubatud, allkirjastatud artefakt; nõutav ressursipiirang; keelatud liiga laiad õigused).
- **B22.** Sama reeglistik, mida jõustab konveier (A18–A20), peab olema jõustatud ka klastri sissepääsu juures, nii et konveierist möödaminnes ei saa reegleid rikkuda.
- **B23.** Käsitsi (konveierist mööda) tehtud muudatused klastris peavad olema kas takistatud või vähemalt tuvastatud ja logitud.

6.6 Identiteet, ligipääs ja saladused

- **B25.** Rakenduse loojal/kasutajal ei tohi olla klastri haldusõigusi; õigused peavad olema rollipõhised (RBAC).
- **B26.** Saladused peavad tulema selleks ettenähtud saladuste haldusest ja jõudma töökoormuseni automaatselt, ilma neid koodi või tõmmisesse kirjutamata (kooskõlas A21–A23).
- **B27.** Volituste rotatsioon peab olema automaatne ja saladuste eluiga piiratud.

6.7 Seire, logimine ja käideldavus

- **B28.** i3 peab pakkuma **tsentraalset logimist, seiret ja häireid (alerting)** nii platvormi kui töökoormuste tasemel.
- **B29.** Platvorm peab võimaldama tuvastada ja teavitada **kahtlasest käitumisest** (nt lubamatu võrguühenduse katse, anomaalne ressursikasutus).
- **B30.** i3 platvormi tasemel tuleb kokku leppida **käideldavuse ootused** (nt hoolduspoliitika, taastumine). PoC-lahenduste puhul ei eeldata toodangutasemega SLA-d, kuid platvorm ise peab olema stabiilne ja isoleeritud tõrgetega.

6.8 Elutsüklil ja kulukontroll

- **B31.** Platvorm peab võimaldama töökoormuste **automaatset elutsükli haldust** — loomine, uuendamine ja **eemaldamine (decommission)**.
- **B32.** PoC-lahendustele peab saama rakendada **aegumist/TTL-i** või sarnast mehhanismi, et vältida kasutusest „zombie“-rakenduste kuhjumist.
- **B33.** Platvorm peab andma **ülevaate olemasolevatest töökoormustest** ja nende omanikest (kataloog/register).
- **B34.** Ressursikvootide ja kulude jälgimine peab olema võimalik töökoormuse/tenandi kaupa.

7. Osa C — Vaikimisi templiit

7.1 Templiidi üldnõuded

- **T1.** Pakkuja kohustus on projekteerida ja tellijale üle anda **vaikimisi templiit**, mida kasutades loodud lahendusi suudab konveier deployda.
- **T2.** Templiit on Tellijale **kohustuslik lähtepunkt** iga uue rakenduse loomisel ning peab olema masinloetavalt seotud konveieri vastavuskontrollidega (policy-as-code, vt A18–A20), nii et templiidist kõrvalekalle on automaatselt tuvastatav ja peatab tarne.
- **T3.** Templiit peab vähemalt katma järgmised nõuded:
 - **Koodi hoidmine** — koodihoidla ja versioonihalduse nõue (kus ja kuidas koodi hoitakse).
 - **Komponendid** — rakenduse loomisel lubatud/eeldatavad tehnoloogiad.
 - **Andmete hoidmine** — millises andmebaasis/lahenduses andmeid hoitakse.
 - **Logimine** — mida ja kuidas rakendus peab logima.
 - **Modulaarsus** — kuidas kood peab olema jaotatud.
 - **Automaattestid** — nõue automaatselt koostatavatele automaattestidele.
 - **Välise API-de kasutamine** — kuidas kasutada väliseid API-sid ja nendega seotud ressursse; siit tuleneb ka eraldi teekide vajadus (nt Vertica ja Teams), et tagada kontrollitud ligipääs.
 - **Rakenduse struktuur** — kuidas rakendus tuleb üles ehitada.
- **T4.** Templiidi koostamisel peab pakkuja lähtuma **parimatest praktikatest** ning **RIKi ja RIA mittefunktsionaalsetest nõuetest**.
- **T5.** Templiit peab olema **versioonihalduses**, dokumenteeritud ja **laiendatav** — nõudeid peab saama ajas täiendada ilma põhistruktuuri ümber tegemata.
- **T6.** Templiit peab olema kavandatud nii, et selle alusel loodud rakenduse hilisem üleandmine arendustiimile ja toodangusse viimine oleks võimalikult väikese ümbertegemisega (kooskõlas C5).
- **T7.** Templiiti peab olema võimalik erinevate lõppkasutajate vibecode-imist võimaldavata tarkvarade puhul (nt Lovable.dev, Claude Code, Cursor).

Alljärgnevad nõuded (T8–T29) suunavad vibecode-itud koodi unifiitseeritud, lihtsate ja jätkusuutlike lahenduste poole ning maandavad AI-genereeritud vigase või liigkeeruka koodi riski. Kõik läviväärtused on kokkulepitavad ja versioonihalduses (kooskõlas A15), nõuded peavad olema jõustatud policy-as-code'ina (vt A18–A20) ning antud AI-le **ette juba templiidis/promptis**, mitte üksnes tagantjärele kontrollitud.

7.2 Lihtsuse ja keerukuse piirid

- **T8.** Funktsiooni **tsüklomaatiline keerukus** ei tohi ületada kokkulepitud läve (nt 10).
- **T9.** Funktsiooni ja faili **pikkusele** kehtivad ülempiirid (nt funktsioon $\leq \sim 50$ rida, fail $\leq \sim 400$ rida), sundides koodi jaotama väiksemateks osadeks.
- **T10.** Kontrollivoo **pesastatuse sügavus** ei tohi ületada kokkulepitud piiri (nt 3–4).

- **T11. Surnud kood** (kasutamata funktsioonid, muutujad, importid) on keelatud ja peab tarne peatama.
- **T12. Koodikorduse (duplikatsiooni)** osakaal ei tohi ületada kokkulepitud läve.

7.3 Sõltuvuste distsipliin

- **T13.** Sõltuvusi tuleb **minimeerida** — eelistada standardteeki; iga uus sõltuvus vajab põhjendust.
- **T14.** Iga deklareeritud sõltuvus peab olema **kasutatud** ja iga kasutatud teek **deklareeritud** (ei tohi olla deklareerimata importe ega kasutuseta sõltuvusi).
- **T15. Lukustusfail (lockfile)** on kohustuslik ja sõltuvuste versioonid peavad olema fikseeritud, et build oleks korratav.
- **T16.** Iga sõltuvus peab **eksisteerima heakskiidetud registris/paketi peeglis** (kooskõlas A10–A11) — see maandab AI hallutsineeritud pakettide riski.

7.4 Arhitektuur ja modulaarsus

- **T17.** Rakenduse **arhitektuur peab olema kirjeldatud koodina** — lubatud komponendid ja nendevahelised lubatud sõltuvused defineeritud masinloetavalt, et arhitektuurist kõrvalekaldeid (drift) saaks automaatselt tuvastada.
- **T18.** Uus rakendus tuleb alglaadida **kohustuslikust standardstruktuurist (scaffold)** — kataloogistruktuur ja kihid on ette antud.
- **T19.** Kehtivad **ühtsed nimetamiskonventsioonid** (failid, muutujad, endpoint'id jne).
- **T20.** Kood peab järgima **kihilist eraldatust (separation of concerns)** — nt äriloogika, andmeligipääs ja liides on eristatud.

7.5 Testimine

- **T21.** Kood peab olema kaetud **automaattestidega, mida konveier suudab automaatselt käivitada** (kooskõlas A16); testideta kood ei läbi konveieri.
- **T22.** Peab olema täidetud **minimaalne testikate lävi** (kokkulepitav) ning iga oluline moodul/endpoint peab olema testidega kaetud.
- **T23.** Testid peavad olema **sisukad** — triviaalsed või tühjad testid ei täida katvuse nõuet.
- **T24.** Muudatused ei tohi rikkuda olemasolevat käitumist — **regressioonitestid** peavad läbima.

7.6 Tüübi- ja staatiline rangus

- **T25. Staatiline tüüpimine** on kohustuslik (tüübitud keel või tüübivihjed) ja tüübikontroll peab läbima.
- **T26. Linter** peab läbima kokkulepitud reeglistiku alusel **ilma hoiatusteta**.

7.7 Loetavus ja dokumentatsioon

- **T27.** Iga rakendusega on kohustuslik **README/kasutusjuhend** (kuidas käivitada, seadistada, testida).
- **T28.** Eelistada tuleb **selget, arusaadavat koodi** „nutika“ asemel; mitteilmne loogika peab olema kommenteeritud — see hõlbustab hilisemat üleandmist arendustiimile.

- **T29. AI-genereeritud osad** peavad olema jälgitavad (märgitud/kommenteeritud) ning kasutatud prompt-mustrid dokumenteeritud organisatsiooni õppimiseks.
-

8. Ühised ja mittefunktsionaalsed nõuded

- **C1. Turvalisus kavandatuna (secure by design):** turvalisus ja isolatsioon peavad olema vaikeseaded, mitte lisavõimalused. Ebaturvaline konfiguratsioon peab olema takistatud, mitte üksnes ebasoovitav.
 - **C2. Vaikekeeld (deny by default):** kõik võrgu- ja ligipääsuõigused on vaikimisi keelatud ja avatakse ainult selgesõnaliselt.
 - **C3. Jälgitavus ja auditeeritavus:** kõik olulised sündmused (deploy, poliitikaotsused, ligipääsud, egress/ingress muudatused) peavad olema logitud ja tagantjärele jälgitavad.
 - **C4. Deklaratiivsus ja korratavus:** nii konveier kui i3 peavad olema kirjeldatud koodina ja taasloodavad ilma käsitsi seadistusega.
 - **C5. Standardiseerimine üleandmise huvides:** lahendus peab kasutama võimalikult samu standardeid ja kontrole, mida kasutatakse toodangus, et hilisem üleandmine arendustiimile oleks võimalikult väikese ümbertegemisega (shift-left).
 - **C6. Dokumentatsioon:** pakkuja peab tarnima arhitektuuri-, kasutus- ja halduskirjelduse ning tööjuhendid (runbook'id) tavaoperatsioonideks ja tõrkeolukordadeks.
 - **C7. Teadmussiire:** pakkuja peab koolitama tellija meeskonda lahenduse iseseisvaks käitamiseks ja edasiarendamiseks. Pakkuja annab tellija enda meeskonnale üle oskused ja teadmise, mida on vaja konveieri ja i3 keskkonna iseseisvaks käitamiseks ja edasiarendamiseks.
 - **C8. Laiendatavus:** lahendus peab võimaldama uute rakenduste, reeglite ja kontrollide lisamist ilma põhiarhitektuuri ümber tegemata.
 - **C9. Vastavus organisatsiooni nõuetele:** lahendus peab arvestama organisatsiooni info-turbe-, andmekaitse- ja vastavusnõuetega, mis täpsustatakse hanke käigus.
-

9. Üleandmise ja vastuvõtu kriteeriumid

Lahendus loetakse vastuvõetuks, kui vähemalt on tõendatud, et:

1. GitHubi lisatud näidiskood läbib konveieri **täisautomaatselt** ja deployb i3 keskkonda ilma käsitsi vahesammudeta (v.a kokkulepitud heakskiidupunktid).
2. Reeglitele **mittevastav** kood (nt keelatud sõltuvus, poliitikarikkumine, ebaõnnestunud test) **peatatakse** ja ei jõua i3-sse — tõendatud negatiivsete testjuhtumitega.
3. Kaks i3-sse deploytud töökoormust on **tõendatavalt isoleeritud** — üks ei pääse teise ressurssidele/andmetele ega mõjuta teise jõudlust (demonstreeritud testiga).
4. Töökoormuse **egress on vaikimisi keelatud** ja avaneb ainult konveieri deklareeritud ulatuses; sisevõrku ei pääse — tõendatud testiga.

5. Rakendus on **vaikimisi ainult sisevõrgust** kättesaadav; välisvõrgust ligipääs on võimalik ainult selgesõnalise erandkorras deploymisega — mõlemad stsenaariumid demonstreeritud.
6. Sama reeglistik on jõustatud **nii konveieris kui klatri sissepääsus** — tõendatud katsega minna konveierist mööda.
7. Tarnitud on nõutav **dokumentatsioon, runbook'id ja teadmussiire**.
8. Pakkuja on üle andnud **vaikimisi templiidi** (Osa C), mis katab nõutud valdkonnad ja on seotud konveieri vastavuskontrollidega; selle alusel loodud näidisarendus läbib konveieri ja deployb i3-sse.

Täpne testjuhtumite komplekt ja vastuvõtuprotokoll lepatakse pakkujaga kokku enne töö käigus.

10. Pakkuja poolt üleantav (deliverables)

1. Töötav CI/CD konveier (Osa A) koos konfiguratsiooni ja taaskasutatava mustriaga.
 2. Töötav i3 pilveskeskkond (Osa B), kirjeldatud koodina ja taasloodav.
 3. Vaikimisi templiit (Osa C) koos dokumentatsiooniga, versioonihalduses ja konveieri vastavuskontrollidega seotud.
 4. Poliitikate/reeglite komplekt (policy-as-code), jõustatud konveieris ja klatri.
 5. Arhitektuuri- ja halduskirjeldus, tööjuhendid (runbook'id), turvakontrollide ülevaade.
 6. Peale punktis 1-5 üleantu vastuvõtmist 40h ulatuses konsultatsioone, et toetada tellijal rakenduste deploymist ning selle käigus tekkivate probleemide lahendamist. Nimetatud tunnid kasutatakse ära 2026a jooksul.
-

11. Eeldused ja piirangud

- Lähtekood asub GitHubis ning organisatsioon tagab selle ja vajalike süsteemide ligipääsu.
- Konkreetsete tootevalikute ettepanek ja põhjendus on pakkuja ülesanne, kui käesolev dokument ei sätesta teisiti. Valitud lahendused tuleb enne töödega alustamist tellijata läbi rääkida.

TÖÖVÕTULEPINGU NR 5-6/5540 ERITINGIMUSED Projekt

Eesti Vabariik, Justiits- ja Digiministeeriumi kaudu, registrikood 70000898, asukoht Suur-Ameerika 1, 10122 Tallinn, keda esindab [ees- ja perekonnanimi] (edaspidi nimetatud „Tellija“) ja

[Jur.isiku või FIE ärinimi], registrikood [number], asukoht [aadress], keda esindab [ees- ja perekonnanimi] (edaspidi nimetatud „Töövõtja“),
edaspidi koos nimetatud „Pooled“ ja eraldi „Pool“,

sõlmisid käesoleva töövõtulepingu (edaspidi „leping“) alljärgnevas:

1. Lepingu objekt

Lepingu objektiks on töövõtja poolt Vibecoding-rakenduste turvalise CI/CD konveieri ja isoleeritud pilvekeskkonna loomine lähtudes väikehanke dokumentidest (edaspidi „tööd“). Tööde täpsem kirjeldus on [toodud lisas 1 – Tehniline kirjeldus].

2. Tööde teostamise aeg ja tähtpäevad

Töövõtja kohustub teostama lepingu objektiks olevad tööd hiljemalt **01.12.2026**. Tööde teostamise täpsem ajakava [lisada sobiv variant, millest nähtub täpsem ajakava]. Pooltel volitatud esindajad võivad kirjalikku taasesitamist võimaldavas vormis lepingu täitmise käigus ajakava täpsustada ja kohandada, muutmata lõpptähtpäeva.

3. Lepingu hind

- 3.1. Lepingu alusel töövõtja poolt teostatavate tööde kogumaksumuseks on **[numbritega] eurot**, millele lisandub käibemaks õigusaktidega sätestatud korras, välja arvatud punktis 3.2 nimetatud juhul (edaspidi nimetatud „lepingu hind“).
- 3.2. Kui pakkumuse esitamise ajal ei olnud töövõtja käibemaksukohustuslane või tal ei olnud kohustust käibemaksu arvestada, kuid selline kohustus tekkis pärast pakkumuse esitamist või lepingu täitmise käigus, peab töövõtja arvestama, et lepingu hind sellest käibemaksu võrra ei suurene.
- 3.3. Lepingu hind on lõplik ja sisaldab kõiki lepingu täitmise kulusid, sh tasu autoriõiguste eest.
- 3.4. Lepingu hind tasutakse pärast töö vastuvõtmist tellija volitatud esindaja poolt. Tasumine toimub poolte allkirjastatud üleandmise-vastuvõtmise akti alusel vastavalt esitatud arvele [ühe maksena peale tööde teostamist].
- 3.5. Töövõtja esitab Tellijale arve e-arvena. E-arvet on võimalik saata e-arvete operaatori vahendusel. E-arve loetakse laekunuks selle operaatorile laekumise kuupäevast.
- 3.6. Tööd rahastatakse []

4. Erisätted

- 4.1. Lisaks üldtingimustes sätestatud kohustub töövõtja:
 - 4.1.1. *esitama aruandluse*;
 - 4.1.2. *järgima lepingu rahastaja tingimusi (sh teavitamisele, vormistamisele ja sümboolikale)*;
 - 4.1.3. pakkumuses esitatud meeskonnaliikmete vahetumise korral tagama, et tööd teostavad vähemalt väikehanke dokumentides nõutud pädevuse ja kogemusega isikud. Meeskonnaliikme vahetumise vajadustest tuleb tellija esindajat teavitada esimesel võimalusel ning esitada uue meeskonnaliikme pädevust ja kogemust tõendavad andmed ja dokumendid. Meeskonnaliikmete vahetamiseks on vajalik tellija nõusolek. Teavitus ja nõusolek esitatakse kirjalikku taasesitamist võimaldavas vormis;
 - 4.1.4. töö teostamisel tegutsema sõltumatu eksperdina ning lähtuma oma parimatest valdkondlikest teadmistest, kogemustest ja meetoditest. Töövõtja kohustub lepingu täitmisel tagama, et mistahes temapoolne äri- või muu tegevus ei ole suunatud kolmandate isikute huvide esindamisele. Käesolevas punktis sätestatud huvide konflikti vältimise kohustuse rikkumise korral on tellijal õigus nõuda töövõtjalt leppetrahvi kuni 20% lepingu hinnast. Samuti on tellijal õigus kirjeldatud juhul leping erakorraliselt ühepoolselt lõpetada.

- 4.2. Lisaks üldtingimustes sätestatud kohustub tellija:
4.2.1. tegema töövõtjale kättesaadavaks kõik tema käsutuses olevad töö teostamiseks vajalikud materjalid, analüüsid vm;
- 4.3. Punktides [viited lepingu punktidele] sätestatud kohustuste rikkumise korral on tellijal õigus nõuda töövõtjalt leppetrahvi [numbritega] eurot.
- 4.4. Töövõtja, sh tema töötaja, ametnik kui temaga mistahes muus lepingulises suhtes olev lepingu täitmisel osalev isik teavitab tellija tööalase tegevusega teatavaks saanud Euroopa Liidu õiguse rikkumisest e-posti aadressil vihje@justdigi.ee. Tellija tagab tööalase tegevusega teatavaks saanud Euroopa Liidu õiguse rikkumisest teavitaja kaitse. Rikkumisest teavitamise ja teavitaja kaitse tagamise õiguslike aluste ning kohustuste rikkumisel kohalduva vastutuse osas lähtuvad pooled [Tööalasest Euroopa Liidu õiguse rikkumisest teavitaja kaitse seaduses](#) sätestatust.
- 4.5. Kui töövõtja ei täida lepingu punkti 4.1.2 nõuetekohaselt ja selle alusel teeb rakendusasutus toetuse vähendamise või tagasinõude otsuse, on tellijal õigus töövõtjalt tagasi nõuda mitteabikõlblikud kulud tagasimakse nõude ulatuses.

5. Volitatud esindajad

- 5.1. Tellija volitatud esindajaks lepingu täitmisega seotud küsimustes on [ees- ja perekonnanimi], tel [number], e-post [aadress], või teda asendav isik.
- 5.2. Töövõtja volitatud esindajaks lepingu täitmisega seotud küsimustes on [ees- ja perekonnanimi], tel [number], e-post [aadress].

6. Lepingu lisad

Lepingu juurde kuuluvad allkirjastamise hetkel lisadena alljärgnevad dokumendid:

- 6.1. Lisa 1 - [lepingu objekti kirjeldus];
6.2. Lisa 2 - [muud vajalikud lisad].

7. Muud sätted

- 7.1. Lepingu osaks on lisaks käesolevatele eritingimustele ja nende lisadele töövõtulepingute üldtingimused. Töövõtja kinnitab, et on üldtingimustega tutvunud paberkandjal või elektroonselt Justiits- ja Digiministeeriumi kodulehel aadressil https://www.justdigi.ee/majandusteave-ja-riigihanked#justiitsministeeriumi_lepingute_uldtingimused ning tal oli võimalik nende kohta küsida selgitusi ja teha ettepanekuid eritingimustes üldtingimuste kohaldamata jätmiseks või muutmiseks. Pooled kinnitavad, et kõik üldtingimused on mõistlikud ega saa seetõttu olla tühiised.
- 7.2. Kui konkreetset sättest ei tulene teisiti, tähendab mõiste „leping” lepingu eritingimusi ja üldtingimusi koos kõikide lisadega. Lepingu dokumentide prioriteetsus on järgmine: eritingimused (I), lepingu lisad (II) ja üldtingimused (III). Vastuolude korral lepingu dokumentide vahel prevaleerib prioriteetsem dokument. Lepingu sõlmimisega kaotavad kehtivuse kõik töövõtja hinnapakumises või muus sarnases dokumendis sisalduvad tingimused niivõrd, kuivõrd need on vastuolus lepingu eritingimuste ja üldtingimustega.
- 7.3. Leping allkirjastatakse digitaalselt.

Tellija

/allkirjastatud digitaalselt/

Tel: 620 8100
E-post: info@justdigi.ee

Töövõtja

/allkirjastatud digitaalselt/

Tel: [number]
E-post: [aadress]