



Rekstrarhandbók

Leiðarvísir fyrir rekstur og
eftirlit stafrænna lausna fyrir
íslenskar heilbrigðisstofnanir

Útgefandi:

Heilbrigðisráðuneytið | Stafræn Heilsa

Rekstrarhandbók

1. ÚTGÁFA | JÚLÍ 2026

sh@hrn.is

<https://stafrænheilsa.is>

Umbrot og textavinnsla:

Heilbrigðisráðuneytið

©2025 Heilbrigðisráðuneytið

ISBN 978-9935-515-96-4

Efnisyfirlit

1. Fyrirvari	7
2. Breytingar frá fyrri útgáfu	8
3. Tilgangur, umfang og ábyrgð	9
3.1 Tilgangur	9
3.2 Áskorunin	9
3.3 Markhópur	9
3.4 Ábyrgðarskipting (RASCI)	10
3.5 Afmörkun gagnvart þróunarhandbók	10
4. Umhverfi og rekstrarumgjörð	12
4.1 Rekstrarumhverfi	12
4.2 Samræmi milli umhverfa	12
4.3 Nafnahefðir	13
5. Skjölun	14
5.1 Markmið og meginreglur	14
5.2 Afmörkun gagnvart þróunarhandbók	14
5.3 Lágmarkskröfur og snið	14
6. Aðgangsstýring, auðkenni og leyndarmál	15
6.1 Aðgangur starfsmanna	15
6.2 Aðgangur verktaka og þjónustuaðila	15
6.3 Þjónustureikningar og vélaaðgangar	16
6.4 Leyndarmálageymsla	16
6.5 Reglur um lykilorð og endurnýjun	16
6.6 Bann og takmarkanir	17
7. Vöktun, mælingar og keyrslustöður	18
7.1 Atvikaskráning (e. Logging)	18

7.2	Rekjanleiki fyrirspurna.....	18
7.3	Mælingar og viðvaranir	19
7.4	Viðvörðunarpöskuldar	19
7.5	Mælaborð.....	19
8.	Þjónustustig og rekstrarlegar skuldbindingar.....	20
8.1	Þjónustustigssamningar (SLA).....	20
8.2	Aðgreining milli umhverfa	20
8.3	Bakvaktir og úthringingar	20
8.4	Viðhaldstímar og útgáfutakmarkanir.....	21
8.5	Afritun.....	21
8.6	Prófanir á endurheimt (e. Restore).....	22
9.	Áætlun um rekstrarsamfellu.....	23
9.1	Innihald viðskiptasamfelluáætlunar	23
9.2	RTO og RPO.....	24
9.3	Prófanir á viðskiptasamfellu	25
9.4	Endurskoðun og viðhald	25
10.	Atvikaskráning og tilkynningar	26
10.1	Alvarleikastig og viðbragðstímar.....	26
10.2	Tilkynningarskyldur eftir alvarleika	26
10.3	Atvikaskráning og meðhöndlun	26
10.4	Stöðuskráning	27
10.5	Eftirfylgni og lærdómur.....	27
11.	Breytinga- og útgáfustjórnun	28
11.1	Samþykktir og ábyrgð.....	28
11.2	Skilyrði fyrir útgáfu í rekstrarumhverfi	28
11.3	Rollback-ferlar	29
11.4	Gagnagrunns- og stillingabreytingar.....	29

11.5	Neyðarbreytingar	29
11.6	Yfirtaka og samningslok.....	30
12.	Viðauki 1: Rekstrarskjölunarkröfur	31
13.	Viðauki 2: Útgáfudagatal	34
14.	Viðauki 3: Verkferill við útgáfu hugbúnaðar	36
15.	Viðauki 4: Gátlistar rekstrar og eftirlits hugbúnaðar	38
16.	Viðauki 5: Ábyrgðarskipting (RASCI)	40

Þessi rekstrarhandbók skilgreinir kröfur, verklag og leiðbeiningar sem snúa að rekstri, eftirliti og vöktun hugbúnaðarlausna og tækniinnviða verkkaupa.

Handbókin er hluti af heildstæðu handbókakerfi og skal lesa hana í samhengi við:

1. Tæknistefna verkkaupa
2. Þróunarhandbók verkkaupa
3. Hönnunarhandbók verkkaupa

Ef árekstur verður milli skjala gildir tæknistefna um tæknilegt val og tæknilegar afstöður. Um þróunarferla, gæðakröfur og skil gildir þróunarhandbók. Um rekstrarferla, vöktun, aðgangsstýringu og þjónustustig gildir rekstrarhandbók þessi.

Allir sem lesa þennan texta eru hvattir til að hugsa gagnrýnið um efni skjalsins og koma með tillögur að úrbótum til verkefnastjóra.

1. Fyrirvari

Rekstrarhandbók þessi er eign verkkaupa og er frekari birting óheimil nema með samþykki.

Kröfur sem settar eru fram í þessari handbók eru bindandi fyrir alla aðila sem koma að rekstri, vöktun og þjónustu hugbúnaðarlausna verkkaupa, þar á meðal innri rekstrarteymi, ytri þjónustuaðila og verktaka.

Hvers kyns notkun á lausnum eða tillögum úr þessari handbók, eins og þær koma fyrir, er á ábyrgð viðkomandi aðila og verkkaupa að skaðlausu.

2. Breytingar frá fyrri útgáfu

Þetta er fyrsta útgáfa rekstrarhandbókarinnar sem sjálfstætt skjal. Rekstrartengdu efni var áður dreift á þróunarhandbók og önnur innri skjöl en hefur verið sameinað í eitt skjal til að skýra ábyrgð, ferla og kröfur sem snúa sérstaklega að rekstri.

Nýtt efni

- Rekstrarhandbók gefin út sem sjálfstætt skjal með eigin fyrirvara og skjalastigveldi.
- Nýr kafli §9: Viðskiptasamfelluáætlun — innihald, RTO/RPO, prófanir, endurskoðun og viðhald.
- Handbókin hefur verið sett í sniðmót HRN.
- Tilvísanir í kafla hafa verið leiðréttar til að passa við kaflanúmer í nýju sniðmóti.

3. Tilgangur, umfang og ábyrgð

3.1 Tilgangur

Rekstrarhandbók þessi setur fram kröfur og ferla sem verkkaupi gerir til reksturs, vöktunar og eftirlits hugbúnaðarlausna og tengdra tækniinnviða. Handbókin er grundvöllur í útboðum og samningum við þjónustuaðila og skal notuð sem viðmið við mat á rekstrargæðum.

Markmiðið er að tryggja fyrirsjáanleika, stöðluð verklag og samfellu í rekstri — óháð breytingum á rekstraraðilum, þjónustuveitendum eða teyimum.

3.2 Áskorunin

Rekstur kerfa verkkaupa er umfangsmikill og kerfin þjóna mikilvægum hlutverkum í heilbrigðisþjónustu. Umhverfi og þarfir breytast hratt og rekstur, hýsing og þjónusta kerfa er útboðsskyld. Skjölun og stöðlun ferla er þar af leiðandi forsenda þess að:

- yfirtaka milli þjónustuaðila gangi snurðulaust fyrir sig,
- kerfin standist úttektar-, öryggis- og eftirlitskröfur settar af eftirlitsaðilum á Íslandi og í Evrópu,
- forvirkri vöktun sé viðhaldið til að tryggja sem mesta uppitíma og skilvirk viðbrögð við truflunum,
- samfella í heilbrigðisþjónustu sé tryggð fyrir alla þjónustuþega og notendur.

3.3 Markhópur

Þessi rekstrarhandbók er ætluð öllum sem koma að rekstri, eftirliti og þjónustu hugbúnaðarlausna verkkaupa:

Markhópur	Hlutverkslýsing
Rekstrarteymi	Dagleg vöktun, viðbrögð við atvikum, viðhald innviða
Öryggisteymi	Öryggiseftirlit, aðgangsstýring, úttektir
Tæknilegir ábyrgðaraðilar	Heildaryfirsýn yfir tæknilausnir og innviði
Verktakar og þjónustuaðilar	Hýsing, rekstur og þjónusta samkvæmt samningum
Stjórnendur	Yfirsýn yfir rekstrarumgjörð, SLA og áhættumat
Útboðsaðilar	Skilgreining krafna í útboðsgögnum

3.4 Ábyrgðarskipting (RASCI)

Til að tryggja skýra ábyrgð, rekjanleika ákvarðana og skilvirkt samstarf skal ábyrgð á helstu rekstrarþáttum skilgreind samkvæmt RASCI-líkani:

Hlutverk	Lýsing
Responsible (R)	Sá aðili sem framkvæmir verkþáttinn
Accountable (A)	Sá aðili sem ber endanlega ábyrgð og tekur ákvörðun
Supportive (S)	Aðilar sem styðja framkvæmd
Consulted (C)	Aðilar sem skulu vera ráðfærðir
Informed (I)	Aðilar sem skulu upplýstir um stöðu og niðurstöður

RASCI-skipting fyrir helstu rekstrarþætti er skilgreind í viðauka 5 (Ábyrgðarskipting).

3.5 Afmörkun gagnvart þróunarhandbók

Rekstrarhandbók og þróunarhandbók skarast á ákveðnum sviðum. Eftirfarandi afmörkun gildir:

Efni	Þróunarhandbók (kaflí)	Rekstrarhandbók (kaflí)
Docker / Kubernetes kröfur	Hvað verksali smíðar (Dockerfile, kube/, probes) — kaflí 18	Hvernig er rekið (vöktun, scaling, afritun, samþykkt útgáfu) — kafla 4, kafla 8
Logging	Hvað lausnin sendir frá sér (structured JSON, ECS, trace IDs) — kaflí 19	Hvert loggar fara, varðveisla, aðgangsstýring — kaflí 7
Útgáfuferli	CI/CD pipeline, gæðahlið, PR-ferli — kaflí 5	Samþykkt í Production, útgáfudagatal, rollback, neyðarbreytingar — kafla 11
Gagnagrunnar	Schema, migrations, Dapper.NET — kaflí 17	Afritun, endurheimtarprófanir, rekstraraðgangur — kaflí 8
Leyndarmál	Vault-samþætting í kóða — kaflí 18	Vault-rekstur, leyndarmálageymsla, endurnýjun — kaflí 6
Mælingar	Endapunktur (/system/metrics) — kaflí 19	Viðvaranir, þröskuldar, bakvaktir — kaflí 7

4. Umhverfi og rekstrarumgjörð

Rekstrarumhverfi hugbúnaðarlausna verkkaupa er hannað með það að markmiði að tryggja stöðugleika, öryggi og fyrirsjáanleika í rekstri, án þess að draga úr sveigjanleika í þróun og samþættingu.

Handbók þessi lýsir rekstrarumgjörð á háu stigi. Nánari tæknileg útfærsla, teikningar og nákvæmar stillingar eru skjalfestar í sérskjölum sem ekki eru birt opinberlega.

4.1 Rekstrarumhverfi

Verkkaupi rekur að lágmarki tvö aðskilin rekstrarumhverfi:

Umhverfi	Lýsing
Sambættingarumhverfi (PreProduction / PPT)	Sambættingar- og prófunarumhverfi sem endurspeglar raunumhverfi eins og kostur er, en er aðskilið netlega og rekstrarlega. Notað fyrir sambættingar, prófanir, útgáfur og sannreyningu áður en breytingar fara í raunumhverfi.
Raunumhverfi (Production)	Raunumhverfi sem þjónar raunverulegum notendum og gögnum og er háð ströngum kröfum um aðgengi, stöðugleika og öryggi.

Notkun PreProduction umhverfis í stað hefðbundins prófunarumhverfis byggir á því markmiði að:

- lágmarka öryggisáhættu tengda gögnum og aðgöngum,
- tryggja sambærilegt rekstrarumhverfi fyrir prófanir og sambættingar,
- styðja við notkun raunhæfra eða nafnlausra (anonymised) gagna eftir því sem við á.

4.2 Samræmi milli umhverfa

Rekstrarumhverfi skal vera einsleitt hvað varðar eftirfarandi þætti, eins og kostur er:

Þáttur	Krafa
Uppsetning þjónustu	Sama uppsetning og stillingar í báðum umhverfum
Gagnagrunnar og tengingar	Sama skema og tengisnið; mismunandi aðgangsupplýsingar
Vöktun og rekjanleiki	Sömu mælingar, loggun og viðvaranir virka í báðum umhverfum
Útgáfuferlar	Sama CI/CD ferli notað fyrir bæði umhverfi; handvirk samþykkt fyrir Production

GitOps	Innviðakóði (Kubernetes manifests, Helm charts) útgáfustýrður og drifinn af GitOps-verkfærum verkkaupa
Statískar framendaeiningar	Leið B framendar (sjá þróunarhandbók kafla 8.2.2) eru afhentar sem statískar skrár (HTML/JS/CSS) og mega keyra í léttum docker-gámi (t.d. nginx, caddy) eða vera afhentar úr.NET bakenda. Slíkir gámar skulu ekki innihalda Node.js runtime og falla undir sömu rekstrarkröfur og aðrir gámar verkkaupa hvað varðar nafnahefðir, útgáfumerkingar og GitOps-samhæfni.

Markmið samræmis er að einfalda rekstur, bilanagreiningu og yfirtöku milli aðila.

Lausnir sem nýta Leið B framenda (þróunarhandbók kafla 8.2.2) geta falið í sér sérstakan docker-gám fyrir stöðugar framendaskrár. Slíkur gámur er létt einföld keyrsla (t.d. nginx eða caddy) sem þjónar statískum skrá og inniheldur ekki Node.js eða annan forritunarmálaþjón (nextjs, integrated frontend-backend frameworks). Gámurinn fellur undir sömu kröfur um nafnahefðir (kafla 4.3), vöktun og útgáfumerki og aðrir gámar verkkaupa. Ef framendinn er afhentur úr.NET bakenda (t.d. wwwroot) þarf engan sérstakan gám og engar breytingar á rekstrarumgjörð.

4.3 Nafnahefðir

Nafnahefðir skulu vera samræmdar og skjalfestar til að tryggja rekjanleika og fyrirsjáanleika.

Þáttur	Regla
Rekstrareiningar (þjónustur)	Skulu fylgja sömu nöfnum og kóðageymslur í GitHub
Gagnagrunnar	Stöðluð nafnasnið sem endurspeglar tegund, umhverfi og tilvik
Kubernetes þjónustur	Heiti þjónustu, namespace-a og annarra auðlinda stöðluð og samræmd milli umhverfa
Vélar og netþjónar	Nafnasnið sem endurspeglar hlutverk, umhverfi og tilvik

Nákvæm nafnasnið og dæmi eru skilgreind í viðauka 1 (Rekstrarskjölunarkröfur) og í sérskjölum verkkaupa sem ekki eru birt opinberlega.

5. Skjölun

5.1 Markmið og meginreglur

Markmið rekstrarskjölunar er að tryggja rekjanleika, yfirsýn og samfellu í rekstri hugbúnaðarlausna verkkaupa — óháð breytingum á rekstraraðilum, þjónustuveitendum eða teymum.

Meginregla	Lýsing
Nægileg en ekki óþarfa ítarleg	Skjölun skal vera nægjanlega ítarleg til að styðja við daglegan rekstur, vöktun og bilanagreiningu, en án þess að birta viðkvæmar tæknilegar upplýsingar í opinberu skjali
Viðhaldshæf	Skjölun skal vera á sniði sem auðvelt er að viðhalda og uppfæra
Ábyrgð	Þjónustuveitendur og rekstraraðilar bera ábyrgð á að viðhalda nákvæmri og uppfærðri skjölun fyrir þann hluta rekstrarumhverfis sem þeir bera ábyrgð á.

5.2 Afmörkun gagnvart þróunarhandbók

Tækniskjölun sem verksali afhendir (README, /Docs, ADR, sequence rit) er skilgreind í þróunarhandbók verkkaupa (kaflí 15). Rekstrarhandbók þessi fjallar um þá skjölun sem snýr sérstaklega að rekstri:

Rekstrarskjölun (þessi handbók)	Tækniskjölun (þróunarhandbók, kaflí 15)
Innvíðateikningar og netuppsetning	README.md og /Docs möppuskipulag
Umhverfislýsingar (PPT, Production)	ADR (arkitektúrakvarðanir)
Aðgangsstýring og leyndarmálaskjölun	Sequence rit og kjarnaflæði
Vöktun, viðvaranir og bakvaktir	Uppsetningarleiðbeiningar
Afritun og endurheimtarferlar	CronJob skjölun
SLA og þjónustustig	Rekstrarskjölun í /Docs (keyrsluumhverfi, stillingar)

5.3 Lágmarkskröfur og snið

Lágmarkskröfur til rekstrarskjölunar, þar á meðal um innihald, myndræna skjölun, nafnahefðir, geymslu, aðgengi og endurskoðunartíðni, eru skilgreindar í viðauka 1 (Rekstrarskjölunarkröfur).

6. Aðgangsstýring, auðkenni og leyndarmál

Þessi kafli fjallar um aðgangsstýringu, auðkenningar og meðhöndlun leyndarmála í tengslum við samskipti milli kerfa og rekstrarumhverfa. Hér er ekki fjallað um hefðbundna notendaaðganga starfsmanna (t.d. AD-notendur eða almenn MFA-innskráning), heldur tæknilega aðganga sem notaðir eru í rekstri hugbúnaðarlausna.

Aðgangsstýring skal byggja á meginreglum um lágmarksaðgang (least privilege) og, eftir því sem við á, zero trust nálgun. Aðgangsstýring skal vera aðgerðamiðuð (claims-based) — heimildir bundnar við aðgerðir en ekki hlutverk. Sjá þróunarhandbók verkkaupa (kafli 12.3) fyrir rökstuðning og nafnasnið heimilda.

6.1 Aðgangur starfsmanna

Krafa	Lýsing
Aðgangur eftir þörfum	Aðgangur skal veittur eftir þörfum starfs og rekstrarhlutverks
Reglubundin endurskoðun	Aðgangar skulu endurskoðaðir reglulega, aldrei sjaldnar en einu sinni á ári
Starfslok eða hlutverkabreyting	Við starfslok eða breytingu á hlutverki skal aðgangur endurskoðaður strax
Endurskoðunarfundir	Reglubundnir fundir skulu haldnir (að lágmarki tvisvar á ári) til að fara yfir aðgangsheimildir, leyndarmál og tengd öryggisatriði.

6.2 Aðgangur verktaka og þjónustuaðila

Krafa	Lýsing
Rökstuðningur	Aðgangur skal einungis veittur ef rekstrarþörf er til staðar og skriflegur rökstuðningur liggur fyrir.
Samþykki	Aðgangur skal veittur í samráði við öryggisstjóra eða að lágmarki tveggja tæknilegra ábyrgðaraðila verkkaupa.
Skráning	Allur aðgangur verktaka skal vera skráður og rekjanlegur
Tímabinding	Aðgangar skulu vera tímabundnir og renna út sjálfkrafa. Ef sjálfvirk útrunning er ekki möguleg skal aðgangur endurskoðaður reglulega.
Samningslok	Aðgangur fellur sjálfkrafa niður í lok samnings

6.3 Þjónustureikningar og vélaaðgangar

Krafa	Lýsing
Þjónustureikningar	Sérstakir reikningar (service accounts) skulu notaðir fyrir vél-til-vélar samskipti; persónubundnir reikningar skulu aldrei notaðir í sjálfvirkni
API-lyklar	API-lyklar skulu vera útgáfustýrðir, tímabundnir og endurnýjanlegir. Hægt skal vera að afturkalla þá án þess að það hafi áhrif á aðra þjónustu.
Skilríki (TLS/SSL)	Skilríki skulu vera skráð, endurnýjunartíðni skilgreind og endurnýjunarferli sjálfvirkir eftir föngum

6.4 Leyndarmálageymsla

Leyndarmál eru geymd í tveimur aðskildum geymslum eftir notkunarviði:

Geymsla	Notkunarvið	Lýsing
Leyndarmálageymsla í keyrsluumhverfi	Hugbúnaður við keyrslu (Kubernetes) og útgáfufarar (CI/CD)	Stýrir leyndarmálum sem hugbúnaður les sjálfvirkir við keyrslu. Aðgangur takmarkaður við þjónustur og sjálfvirka ferla.
Miðlæg leyndarmálageymsla verkkaupa	Öll leyndarmál sem verkkaupi heldur utan um, þ.m.t. aðgangar að eigin kerfum og sameiginlegir aðgangar	Aðgangsstýrð niður á umhverfi (PreProduction, Production). Verktakar fá ekki aðgang nema undir sérstökum kringumstæðum og í samstarfi við öryggisstjóra.

Í leyndarmálageymslum eiga heima: skilríki, lykilorð skilríkja, notendanöfn og lykilorð fyrir utanaðkomandi kerfi, tengistrengir og mikilvægar aðgangsupplýsingar.

6.5 Reglur um lykilorð og endurnýjun

Krafa	Lýsing
Lágmarkslengd	12 stafir að lágmarki
Flækjustig	Hástafir, lágstafir, tölustafir og tákni — í samræmi við öryggisstefnu verkkaupa
Geymsla	Öll lykilorð skulu geymd í miðlægri leyndarmálageymslu og uppfærð þar ef þeim er breytt. Ekki skal stofna nýjar færslur heldur uppfæra viðeigandi færslu.
Endurnýjun	Lykilorð og aðgangsupplýsingar skulu endurskoðuð að lágmarki einu sinni á ári. Reglubundnir endurskoðunarfundir skulu tryggja að endurnýjun fari fram.
Rekjanleiki	Allar breytingar á aðgangsupplýsingum og leyndarmálum skulu vera rekjanlegar

6.6 Bann og takmarkanir

Óheimilt	Lýsing
Leyndarmál í kóða	Lykilorð, lykjar og önnur viðkvæm gögn skulu aldrei vera geymd í kóða, stillingarskrám eða Docker einingum.
Samnýting aðganga	Persónubundnir reikningar skulu ekki samnýttir milli starfsmanna
Ótímabundnir verktakaaðgangar	Allir aðgangar verktaka skulu vera tímabundnir
Óskráðar breytingar	Breytingar á aðgangsheimildum eða leyndarmálum án skráningar og samþykktar
Vinnsla persónuupplýsinga án gagnavinnslusamnings	Þegar þriðji aðili vinnur persónuupplýsingar fyrir hönd verkkaupa skal gagnavinnslusamningur vera til staðar í samræmi við lög nr. 90/2018.

7. Vöktun, mælingar og keyrslustöður

Markmið vöktunar og mælinga er að tryggja stöðugan rekstur, snemmgreiningu frávika og skilvirk viðbrögð við rekstrartruflunum. Vöktun skal byggja á mæligögnum, rekjanleika og stöðluðum keyrslustöðum kerfa. Þróunarhandbók verkkaupa (kafli 19) skilgreinir hvað lausnir skulu senda frá sér (structured logging, mælingar, heilsuendapunktur). Þessi kafli skilgreinir hvernig verkkaupi safnar, vaktar og bregst við þeim gögnum.

7.1 Atvikaskráning (e. Logging)

Verkkaupi rekur tveggja laga loggunarumhverfi:

Lag	Innihald	Aðgangur
Forritaloggur (application logs)	Leggur úr þjónustum og hugbúnaði, í samræmi við kröfur þróunarhandbókar	Innri starfsmenn verkkaupa og ytri verktakar/þjónustuaðilar samkvæmt skilgreindum aðgangsheimildum
Innviðaloggur (infrastructure logs)	Loggur úr Kubernetes, gagnagrunnum, vefþjónum, netbúnaði og öðrum rekstrarinnviðum	Einungis tæknifólk og þjónustuaðilar verkkaupa. Ytri aðilar mega ekki hafa aðgang.

Forritaloggum og innviðaloggum er safnað í miðlæg vöktunarkerfi verkkaupa. Innviðaloggur mega ekki innihalda viðkvæmar upplýsingar sem ekki eru við hæfi ytri aðila.

Krafa	Lýsing
Lágmarks rekjanleiki	Allar log-færslur skulu innihalda lágmarksrekjanleika (trace.id, x-correlation-id) í samræmi við þróunarhandbók
Varðveisla	Varðveislutími logga skal vera skilgreindur og skráður. Varðveislutími getur verið mismunandi eftir umhverfi og tegund logga.
Eyðing	Eyðing logga skal vera sjálfvirk að varðveislutíma loknum.
Leit	Miðlæg leitar- og greiningarvirkni skal vera aðgengileg í vöktunarkerfi

7.2 Rekjanleiki fyrirspurna

Tryggja skal að proxy-þjónar, eldveggir og millistig áframsendi x-forward- og x-correlation-header upplýsingar þannig að hægt sé að rekja ytri fyrirspurnir frá upphafi til enda.

Krafa	Lýsing
Áframsending	Proxy-þjónar og millistig skulu áframsenda rekjanleikahausa (headers) óbreytta
Bann	Proxy-þjónar, eldveggir og millistig mega ekki fjarlægja rekjanleikahausa
Samræmi	Sömu rekjanleikahausar skulu vera í notkun milli allra þjónusta og umhverfa

7.3 Mælingar og viðvaranir

Mælingum skal safnað á stöðluðu sniði og þær notaðar til vöktunar, viðvarana og afkastagreiningar.

Krafa	Lýsing
Mælingar	Mæligögn skulu vera á stöðluðu sniði (Prometheus eða sambærilegt).
Viðvaranir	Viðvaranir skulu byggðar á mæligögnum og trendum, ekki einstökum log-færslum (nema í undantekningartilvikum þar sem mæligögn liggja ekki fyrir).
Keyrslustöðuendapunktur	Keyrslustöðuendapunktur (/system/alive, /system/ready) skulu nýttir til að vakta stöðu og uppitíma þjónustu
Aðgengi mælinga	Mælingaendapunktur (/system/metrics) eiga ekki að vera aðgengilegir af internetinu; einungis innan VPN, innra nets og milli þjónusta

7.4 Viðvörðunarþröskuldar

Viðvörðunarþröskuldar skulu skilgreindir fyrir hverja þjónustu í samráði við rekstrarteymi og tæknilega ábyrgðaraðila.

Að lágmarki skulu viðvaranir vera skilgreindar fyrir:

Þáttur	Dæmi um viðvörun
Uppitími	Þjónusta svarar ekki uppitíma eða heilsuköllum
Svartími	Svartími fer yfir skilgreind mörk
Villuhlutfall	Hlutfall villna í beiðnum fer yfir skilgreind mörk
Auðlindanotkun	CPU eða minnisnotkun fer yfir skilgreind mörk
Gagnagrunnur	Hæg fyrirspurn, tengingarvillur eða afritunarbílun
Skilríki	Skilríki renna út innan skilgreindra tímamarka

Viðvörðunarþröskuldar skulu vera skjalfestir og endurskoðaðir reglulega í samráði við rekstrarteymi.

7.5 Mælaborð

Verkkaupi skal viðhalda mælaborðum sem veita yfirsýn yfir rekstrarstöðu þjónustu. Mælaborð skulu að lágmarki sýna:

- uppitíma og stöðupjónusta,
- svartíma og villuhlutfall,
- auðlindanotkun (CPU, minni),
- Mikilvægar viðvaranir og atvik.

Mælaborð eru í umsjón verkkaupa og engin bein krafa er gerð á verksala um útfærslu þeirra, svo framarlega sem lausnir senda frá sér mæligögn á stöðluðu sniði samkvæmt þróunarhandbók.

8. Þjónustustig og rekstrarlegar skuldbindingar

Til að tryggja fyrirsjáanleika, ábyrgð og samfellu í rekstri hugbúnaðarlausna verkkaupa skulu skýrir þjónustustigssamningar (SLA) liggja fyrir milli þeirra aðila sem koma að rekstri, viðhaldi og hýsingu lausnanna.

8.1 Þjónustustigssamningar (SLA)

Þjónustustigssamningar skulu skilgreina lágmarkskröfur til reksturs og viðbragða og vera hluti af samningum við rekstrar- og þjónustuaðila. Í þjónustustigssamningum skulu að lágmarki koma fram:

Þáttur	Lýsing
Uppitími	Kröfur um uppitíma þjónustu og kerfa, skilgreindar sem hlutfall (t.d. 99,5% / 99,9%)
Viðbragðstímar	Viðbragðstímar við rekstrartruflunum, skilgreindir eftir alvarleikastigi
Ábyrgðarskipting	Ábyrgðarskipting milli aðila við rekstur, viðhald og viðbrögð
Viðurlög	Viðurlög eða afleiðingar ef þjónustustig eru ekki uppfyllt, eftir því sem við á
Samskiptaferlar	Samskipta- og tilkynningarferlar við frávik og truflanir
Mæling	Þjónustustig skulu byggja á mæligögnum og vöktun; mælingar skulu vera aðgengilegar til sannprófunar

8.2 Aðgreining milli umhverfa

Umhverfi	Þjónustustig
Production	Hámarks uppitímakrafa samkvæmt SLA; bakvaktir og úthringingar virkar
PreProduction (PPT)	Lægri uppitímakrafa en Production; viðhaldstímar sveigjanlegri. PPT er ekki rekstrarumhverfi og nýtur ekki sömu skuldbindinga.

8.3 Bakvaktir og úthringingar

Bakvakt eða fyrir fram skilgreint viðbragð skal vera til staðar fyrir allar rekstrartruflanir sem geta haft áhrif á þjónustur verkkaupa eða kerfi sem þriðju aðilar reiða sig á.

Krafa	Lýsing
SLA-tengd	Viðbragð skal vera skilgreint í þjónustustigssamningum
Úthringiferli	Skýrt úthringiferli og stigvaxandi viðbrögð (escalation)
Sérfræðiaðgengi	Viðeigandi sérfræðingar aðgengilegir innan skilgreindra tímamarka
Tengiliðalisti	Uppfærður tengiliðalisti sem nýttur er við úthringingar og samhæfingu

8.4 Viðhaldstímar og útgáfutakmarkanir

Viðhaldstímar og útgáfutakmarkanir skulu skilgreindar fyrir hverja þjónustu eða kerfi. (sjá viðauka)

Krafa	Lýsing
Viðhaldstímar	Fyrir fram skilgreindir, skjalfestir og tilkynntir
Útgáfufrysting	Skilgreind tímabil þar sem útgáfur eru takmarkaðar eða óheimilar (t.d. stórhátíðir og þekktir álagstímar)
Neyðarútgáfur	Heimildir og ferlar fyrir neyðarútgáfur innan frystingartímabila
Útgáfudagatal	Skal vera hluti af þjónustustigssamningum eða viðeigandi viðaukum (sjá viðauka — Útgáfudagatal).
Tilkynningar til notenda	Fyrirhuguð viðhaldstímabil og þekktar truflanir skulu tilkynnt notendum og hagsmunaaðilum með hæfilegum fyrirvara

8.5 Afritun

Afritun skal tekin af öllum gagnagrunnum og öðrum rekstrarlega mikilvægum gögnum sem verkkaupi á eða ber ábyrgð á.

Tíðni afritunar

Umhverfi	Afritunargerð	Lágmarkstíðni
PreProduction (PPT)	Heildarafrit	Einu sinni í mánuði
Production	Breytingaafrít (differential)	Daglega
Production	Heildarafrit	Einu sinni í viku

Varðveisla afrita skal vera í samræmi við gildandi samninga og kröfur um hýsingu og gagnavinnslu.

Innihald afritunar

Eftirfarandi atriði skulu að lágmarki vera innifalin í afritun:

Þáttur	Lýsing
Gagnagrunnar	Allir gagnagrunnar í viðkomandi umhverfi
Stillingaskrár	Stillingar netþjóna, proxy-þjóna, DNS, VPN og netbúnaðar
Kubernetes	Stillingaskrár rekstrarumhverfis, þjónustur og innviðir
Leyndarmál	Afrit af leyndarmálageymslum (Vault o.þ.h.)
Skilríki	TLS/SSL-skilríki og tengd gögn
Sjálfvirkniskriptur	Skriptur og önnur sjálfvirknivæðing sem tengist reglulegum rekstri

Rekstraraðilar eru hvattir til að bæta við frekari þáttum sem þeir telja nauðsynlega til að tryggja farsæla endurheimt.

8.6 Prófanir á endurheimt (e. Restore)

Endurheimt afrita skal prófuð reglulega til að tryggja heilindi gagna og raunhæfa endurheimtargetu.

Krafa	Lýsing
Reglulegar prófanir	Endurheimtarferli prófað með sjálfvirkum eða hálf sjálfvirkum ferlum eftir því sem við á
Heilindi gagna	Prófanir skulu staðfesta að endurheimt gögn séu heil og nothæf
RTO/RPO	Prófanir skulu styðja við skilgreind endurheimtarmarkmið (Recovery Time Objective / Recovery Point Objective).
Tímamörk	Þjónustuaðili skal tryggja að gögn séu aðgengileg til endurheimtar innan skilgreindra tímamarka
Skjalfesting	Niðurstöður endurheimtarprófana skulu vera skjalfestar

9. Áætlun um rekstrarsamfellu

Verkkaupi skal viðhalda heildstæðri viðskiptasamfelluáætlun (e. business continuity plan) sem nær yfir öll rekstrarkerfi og tækniinnviði. Áætlunin tengir saman þá ferla sem skilgreindir eru í öðrum köflum þessarar handbókar í eitt samræmt viðbragðskerfi og tryggir að allir aðilar sem koma að rekstri viti hlutverk sitt og ábyrgð ef alvarlegar truflanir verða.

Viðskiptasamfelluáætlun er stefnuskjal verkkaupa, ekki verkefnisbundið skjal. Hún er viðhaldin af verkkaupa og þjónustuaðilar bera ábyrgð á að þekkja hana og fara eftir þeim hlutum hennar sem snerta þeirra ábyrgðarsvið.

9.1 Innihald viðskiptasamfelluáætlunar

Viðskiptasamfelluáætlun skal að lágmarki fjalla um eftirfarandi:

Þáttur	Lýsing	Tengsl við aðra kafla
Gildissvið og forgangs röðun	Kerfi og þjónustur sem áætlunin nær yfir eru flokkuð eftir mikilvægi fyrir heilbrigðisþjónustu. Kerfi sem hafa bein áhrif á öryggi sjúklinga eða meðferðarsamfellu skulu hafa hæsta forgang.	—
Áhættumat	Skilgreining á helstu áhættuþáttum sem geta valdið truflunum (tæknibílanir, mannlegir þættir, ytri ógnir, birgjaáhætta). Áhættumat skal vera skjalfest og endurskoðað reglulega.	—
Viðbragðsferlar meðan á truflunum stendur	Virkjun úthringiferla, samskipti við notendur og hagsmunaaðila, uppfærsla stöðusíðu, bráðaaðgerðir til að takmarka áhrif.	§8.2 (Bakvaktir), §10 (Atvikaskráning og tilkynningar)
Endurheimt þjónustu	Rollback-aðgerðir, gagnaendurheimt úr afritum, staðfesting á heilindum gagna, stigvaxandi endurræsing þjónustu. Endurheimtartímamarkmið (RTO) og gagnatapsmarkmið (RPO) skulu vera skilgreind fyrir hvert kerfi eftir mikilvægi.	§8.5 (Afritun), §8.6 (Prófanir á endurheimt), §11.3 (Rollback-ferlar)
Rannsókn eftir atvikum	Formleg eftirfylgni (post-mortem) samkvæmt skilgreindum ferlum, þar á meðal grunnorsakagreining, áhrifamat, úrbótaáætlun og uppfærsla á vöktun og ferlum.	§10.5 (Eftirfylgni og lærdómur)
Tilkynningarferlar	Tilkynning til viðeigandi öryggisaðila (t.d. CERT-IS, Persónuvernd) ef atvik varðar öryggisbrest, gagnaleka eða annað sem tengist persónuvernd eða öryggi	§10.2 (Tilkynningarskyldur eftir alvarleika)

	mikilvægra innviða. Tilkynningarskylda samkvæmt lögum nr. 78/2019 (öryggi mikilvægra innviða), lögum nr. 90/2018 (persónuvernd) og lögum nr. 132/2020 (lækningatæki) eftir því sem við á.	
Tengiliðir og ábyrgðarskipting	Skýr skipting ábyrgðar milli verkkaupa, rekstraraðila, þjónustuaðila og verktaka. Uppfærður tengiliðalisti fyrir öll atvik.	Viðauki 5
Samskiptaáætlun	Hvernig og hvenær innri og ytri aðilar eru upplýstir, hvaða samskiptaleiðir eru notaðar og hver ber ábyrgð á samskiptum á hverju stigi.	§10.4 (Stöðuskráning)

9.2 RTO og RPO

Endurheimtartímamarkmið (Recovery Time Objective, RTO) og gagnatapsmarkmið (Recovery Point Objective, RPO) skulu vera skilgreind fyrir hverja þjónustu eða kerfisheild sem viðskiptasamfelliáætlun nær yfir.

Viðmið	Krafa
RTO	Hámarkstími frá truflunarupphafi til endurreistrar þjónustu skal vera skilgreindur fyrir hvert kerfi og endurspeгла mikilvægi þess fyrir heilbrigðisþjónustu.
RPO	Hámarksgagnatap sem er ásættanlegt, mælt í tíma frá síðasta afriti. Skal endurspeгла afritunartíðni (sjá §8.5) og eðli gagna.
Forgangsöröðun	Kerfi sem hafa bein áhrif á öryggi sjúklinga eða meðferðarsamfelli skulu hafa styttri RTO og RPO en stoðkerfi.
Samræmi við SLA	RTO og RPO skulu vera samræmd við þjónustustigssamning (sjá §8.1) og afritunarstefnu (sjá §6.4).
Prófanir	Endurheimtarprófanir (sjá §8.5) skulu sannreyna að skilgreindum RTO og RPO-markmiðum sé náð í reynd.

Nákvæm gildi RTO og RPO eru skilgreind í þjónustustigssamningum eða viðeigandi viðaukum hvers verkefnis og geta verið mismunandi eftir kerfum.

9.3 Prófanir á viðskiptasamfelli

Viðskiptasamfelliáætlun skal prófuð reglulega til að tryggja að ferlar, tengiliðir og tæknilausnir virki í reynd.

Krafa	Lýsing
Tíðni	Að lágmarki árlega. Oftar ef verulegar breytingar verða á kerfum eða innviðum.

Umfang	Prófanir skulu ná til endurheimtar gagna, virkjunar viðbragðsferla og samskiptaáætlunar.
Skjölun	Niðurstöður prófana skulu skjalfestar og nýttar til úrbóta á áætluninni.
Pátttaka þjónustuaðila	Viðeigandi þjónustuaðilar og rekstraraðilar skulu taka þátt í prófunum eftir því sem ábyrgðarsvið þeirra krefst.

9.4 Endurskoðun og viðhald

Krafa	Lýsing
Reglubundin endurskoðun	Áætlun um viðskiptasamfellu skal endurskoðuð að lágmarki árlega.
Endurskoðun við breytingar	Áætlun skal endurskoðuð þegar veruleg breyting verður á kerfum, innviðum, þjónustuaðilum eða rekstrarumhverfi.
Endurskoðun eftir atvikum	Eftir hvert alvarlegt (CRITICAL) atvik skal meta hvort áætlunin þarfnist uppfærslu.
Ábyrgð	Verkkaupi ber ábyrgð á viðhaldi áætlunarinnar. Þjónustuaðilar bera ábyrgð á að upplýsa um breytingar sem geta haft áhrif á hana.
Útgáfustýring	Áætlunin skal vera útgáfustýrð og skráð hvenær hún var síðast endurskoðuð og af hverjum.

10. Atvikaskráning og tilkynningar

Atvik telst vera hvers kyns ófyrirséð truflun á þjónustu, frávik frá eðlilegri keyrslu kerfa, öryggisbrestur eða óheimill aðgangur sem getur haft áhrif á rekstur, öryggi notenda eða þjónustu verkkaupa.

Markmið atvikaskráningar er að tryggja skjót viðbrögð, skýra ábyrgð, rekjanleika og lærdóm til framtíðar.

10.1 Alvarleikastig og viðbragðstímar

Alvarleiki	Lýsing	Viðbragðstími
Critical	Kerfi óaðgengilegt eða veruleg röskun á þjónustu. Hefur bein áhrif á notendur eða heilbrigðisþjónustu.	Viðbrögð strax; úthringiferli virkjað samkvæmt SLA
Medium	Skert virkni eða hluti þjónustu óaðgengilegur. Takmörkuð áhrif á notendur.	Viðbrögð innan skilgreindra tímamarka samkvæmt SLA
Mild	Engin bein áhrif á notendur. Frávik sem krefst eftirfylgni en ekki tafarlausra aðgerða.	Skráð og meðhöndlað innan eðlilegs rekstartíma

Flokkun atvika skal vera samræmd og notuð til að stýra viðbragðstíma, úthringingum og samskiptum.

10.2 Tilkynningarskyldur eftir alvarleika

Alvarleiki	Innri tilkynning	Ytri tilkynning
Critical	Tæknilegir ábyrgðaraðilar, öryggisstjóri og stjórnendur strax	Stöðusíða uppfærð; notendur og hagsmunaaðilar upplýstir. Ef öryggisbrestur: tilkynning til viðeigandi eftirlitsaðila (t.d. Persónuverndar, CERT-IS) samkvæmt lögum.
Medium	Rekstrarteymi og tæknilegir ábyrgðaraðilar	Stöðusíða uppfærð ef áhrif á notendur
Mild	Rekstrarteymi	Engin ytri tilkynning

10.3 Atvikaskráning og meðhöndlun

Öll atvik skulu skráð á miðlægan hátt og meðhöndluð samkvæmt skilgreindum ferlum.

Atvikaskráning skal að lágmarki innihalda:

Svæði	Lýsing
Lýsing	Lýsing á atviki og áhrifum þess
Tímasetningar	Upphaf, greining, lausn og lokun

Alvarleikastig	Flokkun samkvæmt kafla 10.1
Viðbrögð og aðgerðir	Hvað var gert og af hverjum?
Ábyrgðaraðili	Hver bar ábyrgð á meðhöndlun
Grunnorsök	Greining á orsök atviks (ef þekkt)

Atvikaskráning, skýrslugerð og eftirfylgni skal vera í samræmi við kröfur öryggisstjóra verkkaupa og gildandi gæðahandbók.

10.4 Stöðuskráning

Verkkaupi heldur úti stöðusíðu sem veitir yfirlit yfir rekstrarstöðu þeirra kerfa sem þjónustuð eru.

Krafa	Lýsing
Uppfærsla	Stöðusíða uppfærð í samvinnu rekstarteymis og þjónustuaðila
Innihald	Upplýsingar um rekstartengd atvik, stöðu þeirra og úrlausnir
Samskipti	Nýtt til samskipta við notendur og aðra hagsmunaaðila eftir því sem við á

Tilkynningar og samskipti við atvik skulu vera í samræmi við skilgreinda samskipta- og viðbragðsferla.

10.5 Eftirfylgni og lærdómur

Við öll Critical atvik og endurtekin Medium atvik skal fara fram eftirfylgni (post-mortem) með það að markmiði að draga úr líkum á endurtekningu.

Krafa	Lýsing
Grunnorsök	Greining á raunverulegri orsök atviks (root cause analysis)
Úrbótaáætlun	Skýrar aðgerðir til að koma í veg fyrir endurtekningu
Rekstrarferlar	Niðurstöður nýttar til að bæta rekstrarferla
Vöktun	Viðvaranir og vöktun uppfærð ef atvik leiddi í ljós blinda bletti
Skjölun	Viðeigandi skjöl endurskoðuð og uppfærð
Tímamörk	Post-mortem skal vera lokið innan tveggja vikna frá lokun atviks

11. Breytinga- og útgáfustjórnun

Markmið breytinga- og útgáfustjórnunar er að tryggja stöðugan rekstur, rekjanleika og lágmörkun áhættu þegar breytingar eru gerðar á hugbúnaði og tengdum innviðum verkkaupa.

Þróunarhandbók verkkaupa (kafli 18) skilgreinir tæknilega útfærslu útgáfufarla, CI/CD-sjálfvirknivæðingu og Docker/Kubernetes-kröfur. Þessi kafli skilgreinir rekstrarlegar samþykktir, skilyrði og viðbrögð.

11.1 Samþykktir og ábyrgð

Krafa	Lýsing
Samþykkt í Production	Samþykki útgáfu í Production er ávallt handvirk og á ábyrgð verkkaupa.
Ytri aðilar	Ytri verktakar eða þjónustuaðilar hafa ekki heimild til að samþykkja eða framkvæma útgáfur í Production
Beiðni um breytingu	Verksali eða þjónustuaðili sendir formlega beiðni um útgáfu. Tæknilegir ábyrgðaraðilar verkkaupa meta og samþykkja.
Rekjanleiki	Allar samþykktir skulu vera rekjanlegar og skjalfestar

11.2 Skilyrði fyrir útgáfu í rekstrarumhverfi

Áður en breytingar eða útgáfur eru teknar í notkun í rekstrarumhverfi skulu eftirfarandi skilyrði vera uppfyllt:

Skilyrði	Lýsing
Útgáfudagatal	Útgáfa fylgir skilgreindu útgáfudagatali; frysting virt (sjá kafla 8.4 og viðauka 2 — Útgáfudagatal).
Prófanir og samþykktir	Nauðsynlegar prófanir og samþykktir hafa farið fram samkvæmt þróunarhandbók
Gæðahlið	Allir sjálfvirkir gæðaferlar standast
Vöktun	Vöktun, bakvaktir og viðbragðsferlar eru virkir
Rollback	Endurheimtar- og rollback-ferlar liggja fyrir og hafa verið prófaðir
Tilkynning	Viðeigandi aðilar hafa verið upplýstir um fyrirhugaða útgáfu

11.3 Rollback-ferlar

Fyrir hverja útgáfu í Production skal rollback-ferli liggja fyrir:

Krafa	Lýsing
Skjalfesting	Rollback-ferli skal vera skjalfest áður en útgáfa fer fram
Prófun	Rollback-ferli skal vera prófað í PreProduction áður en útgáfa fer í Production
Tímamörk	Skilgreina skal hámarkstíma frá greiningu vandamáls til þess að rollback er virkjaður
Gagnagrunnur	Ef gagnagrunnsbreytingar fylgja útgáfu skal rollback-ferli taka tillit til backward-compatibility krafna (sjá þróunarhandbók, kafla 17).
Ábyrgð	Tæknilegir ábyrgðaraðilar verkkaupa bera ábyrgð á ákvörðun um rollback

11.4 Gagnagrunns- og stillingabreytingar

Breytingar á gagnagrunnum, stillingum og leyndarmálum skulu fara fram í samræmi við þróunarhandbók og með viðeigandi samþykktum.

Krafa	Lýsing
Afrit	Afrit skal tekið áður en breytingar eru framkvæmdar
Backward-compatibility	Gagnagrunnsbreytingar skulu vera afturvirkir samhæfðar þannig að eldri útgáfa hugbúnaðar virki með nýju skema (sjá þróunarhandbók, kafla 17).
Sannreyning	Sannreyna skal að breytingar valdi ekki truflun á eldri útgáfum hugbúnaðar
SQL-skipanir	Verktakateymi skulu afhenda SQL-skipanir sem uppfæra gagnagrunn í nýja útgáfu, þar á meðal gögn sem þarf til að nýtt skema virki

11.5 Neyðarbreytingar

Neyðarbreytingar eru einungis heimilar við alvarleg rekstrar- eða öryggisatvik (Critical samkvæmt kafla 10.1).

Krafa	Lýsing
Frávik frá ferlum	Má víkja frá hefðbundnum ferlum eftir atvikum
Samþykki	Tæknilegur ábyrgðaraðili verkkaupa skal samþykkja neyðarbreytingu, jafnvel utan hefðbundins vinnutíma
Skjalfesting	Allar breytingar skulu skjalfestar í kjölfar atviks, þar á meðal rökstuðningur fyrir frávik.

Eftirfylgni	Endurskoðun og eftirfylgni skal fara fram samkvæmt kafla 10.5 (post-mortem).
Rekjanleiki	Undantekningar frá skilgreindum ferlum skulu vera rökstuddar og rekjanlegar

11.6 Yfirtaka og samningslok

Úttektaráætlun (exit plan) skal vera hluti af samningsgögnum og endurskoðuð reglulega í samræmi við þjónustustigssamning (sjá §8.1). Við samningslok eða skipti á þjónustuaðila skal fylgja úttektaráætlun og tryggja rekstrarsamfellu í samræmi við tæknistefnu verkkaupa.

Viðauki 1: Rekstrarskjölunarkröfur

Markmið rekstrarskjölunar er að tryggja að tæknifólk, rekstrarteymi og þjónustuaðilar hafi nægilegar upplýsingar til daglegs reksturs, bilanagreiningar og yfirtöku — óháð breytingum á starfsfólki eða þjónustuaðilum.

Lágmarkskröfur til rekstrarskjölunar

Eftirfarandi atriði skulu vera skjalfest fyrir hvert rekstrarumhverfi (PreProduction og Production):

Flokkur	Lágmarksinnihald
Yfirlitslýsing	Lýsing á umhverfi, hlutverki þess og helstu íhlutum
Myndrænt yfirlit	Yfirlitsmynd af arkitektúr, tengingum og ábyrgðarskiptingu. Myndir skulu vera í viðhaldshæfu sniði (draw.io, Visio eða sambærilegt) og merktar útgáfunúmeri, dagsetningu og ábyrgðaraðila.
Þjónustur	Listi yfir þjónustur, hlutverk þeirra og tengsl við önnur kerfi
Netuppsetning	Tengingar, eldveggir, DMZ, VPN, proxy — sýnt á myndrænu yfirliti
Gagnagrunnar	Nafn, tegund, umhverfi, hýsingarstaður
DNS og lén	Öll domain og subdomain í notkun; hvort sem þau eru aðgengileg utan eða innan nets verkkaupa
Skilríki (TLS/SSL)	Hvaða skilríki eru notuð, hvaðan þau koma, endurnýjunartíðni
Aðgangsstýring	Hvernig aðgangi er háttað, hvaða teymi / hlutverk hafa aðgang
Vöktun og viðvaranir	Hvaða mælingar og viðvaranir eru virkar, hvert viðvaranir fara?
Afritun	Afritunarferli, tíðni, varðveislutími og endurheimtarferli

Tvær teikningar — tveir markhópar

Myndræn rekstrarskjölun skal vera aðgengileg á tveimur stigum:

Stig	Markhópur	Innihald
Hátt stig (yfirlit)	Stjórnendur og stefnumótun	Einföld yfirlitsmynd sem sýnir helstu kerfi, tengingar og ábyrgðarskiptingu.
Tæknilegt stig	Rekstrar- og tækniteymi	Nákvæm tæknimynd með eldveggjum, beinum, VLAN, VPN, proxy og gagnaflæði

Gott er einnig að hafa flæðirit (data flow diagram) sem sýnir hvernig beiðnir ferðast í gegnum kerfið (notandi → proxy/VPN → Kubernetes → gagnagrunnur).

Aðgreining umhverfa í myndum

Teikningar skulu sýna greinilega aðgreiningu milli PreProduction og Production umhverfa:

- Litamerkingar eða rammi sem aðgreinir umhverfi
- Hvaða þjónustur keyra í hvoru umhverfi?
- Hvaða aðgangur og netleiðir (VPN, proxy) tengjast hvoru umhverfi?
- Ef sameiginlegir þættir eru milli umhverfa (t.d. gagnasöfn, eldveggir og proxy) skal sýna þá með sameiginlegum hnútum

Nafnahefðir Gagnagrunnar

Nafnasnið: <forskeyti><DBTYPE><ENV><INSTANCE>

Dæmi	Lýsing
emlmssqlstg01	MSSQL grunnur í staging umhverfi, tilvik 01
emlmssqlprd03	MSSQL grunnur í production umhverfi, tilvik 03
emlmssqldev02	MSSQL-grunnur í development/testing umhverfi, tilvik 02

Forskeyti ákvarðast af verkkaupa og getur breyst milli kerfa.

Kubernetes þjónustur

Regla	Lýsing
Samræmd heiti	Heiti þjónustu, namespace-a og annarra auðlinda skulu vera stöðluð
Samræmi milli umhverfa	Sama heiti þjónustu í öllum umhverfum, eftir því sem við á

Tengsl við kóðageymslur	Heiti rekstrareininga skulu fylgja sömu nöfnum og kóðageymslur í GitHub
-------------------------	---

Vélar og netþjónar

Vélar, sýndarvélar og netþjónar skulu fylgja sambærilegu nafnasniði og gagnagrunnar, þannig að heiti endurspegli hlutverk, umhverfi og tilvik.

Nánari útfærsla á nafnahefðum fyrir vélar og netþjóna er skilgreind í sérskjölum verkkaupa.

Geymsla og viðhald rekstrarskjala

Krafa	Lýsing
Geymsla	Skjöl skulu geymd í miðlægum gagnageymslum eða kóðageymslum verkkaupa (t.d. infrastructure GitHub-geymslum undir Docs/).
Útgáfustýring	Skjöl skulu vera merkt útgáfunúmeri og dagsetningu; eldri útgáfur varðveittar
Aðgangur	Aðgengileg innri starfsmönnum og viðeigandi þjónustuaðilum samkvæmt skilgreindum aðgangsheimildum
Viðkvæm skjöl	Skjöl sem innihalda viðkvæmar eða tæknilega nákvæmar upplýsingar geymd í aðgreindum geymslum og ekki birt opinberlega

Endurskoðun

Krafa	Tíðni
Rekstrarhandbók	Endurskoðuð að lágmarki einu sinni á ári
Myndræn skjölun	Yfirfarin að lágmarki tvisvar á ári í samstarfi við rekstrar- og þjónustuaðila
Við meiriháttar breytingar	Viðeigandi skjöl uppfærð án tafar
Eldri útgáfur	Varðveittar í útgáfusögu ásamt dagsetningum og ábyrgðaraðila

Viðauki 2: Útgáfudagatal

Öll verkefni skulu fylgja útgáfudagatali sem skilgreinir þau tímabil þar sem útgáfur eru takmarkaðar eða óheimilar í rekstrarumhverfi (útgáfufrysting / deployment freeze). Þetta er nauðsynlegt til að forðast óþarfa útköll, lágmarka truflun á fyrirsjáanlegum álagstímum og tryggja nægilega mönnun við útgáfu.

Hvert kerfi skal útfæra sitt eigið útgáfudagatal sem inniheldur þær uppitímakröfur eða útgáfufrystingar sem skipta máli fyrir viðkomandi kerfi.

Almennar reglur

Regla	Lýsing
Föstudagar og helgar	Forðast skal útgáfur á föstudögum eða um helgar nema brýn nauðsyn sé
Frídagar	Forðast skal útgáfur stuttu fyrir almenna frídaga eða löng frítímabil þar sem fyrirsjáanlegt er að fámennt verður
Sumarfrítími	Forðast skal útgáfur á sumarfrítíma (júní–ágúst) nema brýn nauðsyn sé
Álagstímar	Kerfi sem þjóna heilbrigðisþjónustu skulu skilgreina sérstaka álagstíma (t.d. flensuvertíð eða hátíðir) þar sem útgáfur eru takmarkaðar
Neyðarútgáfur	Neyðarútgáfur (hotfix) eru undanþegnar frystingu en skulu fylgja neyðarbreytingaferli (sjá §11.5).

Útfærsla

Útgáfudagatal skal vera:

- hluti af þjónustustigssamningum eða viðeigandi rekstrargögnum,
- endurskoðað árlega í samráði við rekstrar- og verkefnateymi,
- aðgengilegt öllum aðilum sem koma að útgáfum.

Verkkaupi útvegar sniðmát fyrir útgáfudagatal. Kerfisstjórar og verkefnastjórar bera ábyrgð á að fylla út og viðhalda dagatali fyrir sín kerfi.

Sniðmát

Eftirfarandi töflu má nota til hliðsjónar en hún inniheldur merkingar fyrir þau tímabil sem almennt ættu að vera skilgreind sem fastafrystingar ■ eða sem breytileg frysting ■ (t.d. kringum breytilega frídaga, s.s. páska).

Janúar	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Febrúar	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29		
Mars	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Apríl	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
Máí	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Júní	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
Júlí	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Ágúst	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
September	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
Október	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Nóvember	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
Desember	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Viðauki 3: Verkferill við útgáfu hugbúnaðar

Þessi viðauki lýsir stöðluðum verkferli við útgáfu hugbúnaðar í PreProduction (PPT) eða Production umhverfi. Ferlið á við um allar útgáfur sem fela í sér hugbúnaðarbreytingar og/eða gagnagrunnsbreytingar.

Verkferlið í skrefum

Skref	Aðgerð	Ábyrgð
1. Afritun	Afrit tekið af gagnagrunni eða viðeigandi gögnum áður en breytingar eru gerðar	Rekstrarteymi verkkaupa
2. Gagnagrunnsbreytingar	SQL-skipanir keyrðar á umhverfi. Gagnagrunnsteymi verkkaupa hefur yfirumsjón og kallar til þjónustuaðila gagnagrunnsreksturs ef þarf.	Gagnagrunnsteymi verkkaupa
3. Sannreying eldri útgáfu	Verkefnastjóri staðfestir að eldri útgáfa hugbúnaðar virki enn á nýju gagnagrunnsskema	Verkefnastjóri verkkaupa
4. Hugbúnaðarútgáfa	Hugbúnaðaruppfærsla keyrð af sjálfvirkum útgáfuflerum. Tæknilegir ábyrgðaraðilar verkkaupa samþykkja útgáfu.	Tæknilegir ábyrgðaraðilar verkkaupa
5. Sannreying nýrrar útgáfu	Verkefnastjóri staðfestir að nýr hugbúnaður virki sem skyldi á nýjum gagnagrunni	Verkefnastjóri verkkaupa
6. Lok og skjölun	Útgáfu lokið; viðeigandi útgáfuskjöl uppfærð	Verkefnastjóri verkkaupa

Kröfur til gagnagrunnsbreytinga

Verktakateymi skulu afhenda SQL-skipanir sem uppfæra gagnagrunn í nýja útgáfu, þar á meðal gögn sem þarf til að nýtt skema virki (ef þörf er á slíku).

Gagnagrunnsbreytingar á kerfi sem er í keyrslu skulu vera afturvirkt samhæfðar (backward-compatible). Eftirfarandi er óheimilt:

Óheimil breyting	Lýsing
Endurskýra dálka	Breyta nafni dálks í töflum eða views
Breyta gagnatýpum	Breyta gagnatýpum eða stytta lengd dálka
Breyta heiti taflna/views	Endurnefna töflur eða views
Fella út dálka	Fjarlægja dálka úr töflum eða views

Fella út lykla	Fjarlægja foreign eða primary lykla þar sem gagnaósamræmi myndi myndast
----------------	---

Þessar kröfur eru í samræmi við þróunarhandbók verkkaupa (kafli 17).

Rollback

Ef vandamál koma upp eftir útgáfu skal rollback-ferli virkjað samkvæmt §11.3 í meginmáli. Afrit sem tekið var í skrefi 1 er forsenda rollback.

Viðauki 4: Gátlistar rekstrar og eftirlits hugbúnaðar

Þessi gátlisti tekur til rekstrarlegra atriða sem ekki eru hluti af þróunarhandbók. Hann skilgreinir kröfur til undirbúnings, vöktunar, viðbragða og langtímareksturs hugbúnaðarlausna í rekstrarumhverfum verkkaupa.

Undirbúningur rekstrar (fyrir PreProduction / Production)

Rekstrarumhverfi

- Rekstrarumhverfi (PreProd / Prod) uppsett og staðfest (**Verkkaupi**)
- Namespace, netreglur og aðgangsstýringar skilgreindar (**Verkkaupi**)
- Leyndarmálageymsla virk og tengd lausn (**Verkkaupi**)

Aðgangar og auðkenningar

- Auðkenningarleið valin og virk (**Verkkaupi**)
- MFA virk þar sem við á (**Verkkaupi**)
- Aðgangsheimildir skilgreindar og prófaðar (**Verkkaupi**)

Vöktun, mælingar og logging

Mælingar og viðvaranir

- Mæligögn tengd miðlægu vöktunarkerfi (**Verkkaupi**)
- Viðvörðunarpöskuldar skilgreindir (CPU, minni, svartími, villur) (**Verkkaupi**)
- Viðvaranir prófaðar (**Verkkaupi**)

Logging

- Forritalögum safnað í miðlægt kerfi (**Verkkaupi**)
- Innviðalöggum safnað í aðgreint kerfi (**Verkkaupi**)
- Varðveisla og eyðing logga skilgreind (**Verkkaupi**)

Rekjanleiki og stöðueftirlit

- /version endapunktur nýttur í vöktun og sannreyningu (**Verkkaupi**)
- /system/alive og /system/ready tengd sjálfvirkri endurræsingu (**Verkkaupi**)
- Rekjanleikahausar (trace.id, x-correlation-id) eru staðfestir í gegnum alla þjónustukeðju (**Verkkaupi**).

Útgáfur og breytingastjórnun

- Útgáfudagatal skilgreint (sjá viðauka 2 — Útgáfudagatal) (**Verkkaupi**)
- Ferli fyrir neyðarútgáfur (hotfix) skilgreint (sjá §11.5) (**Verkkaupi**)
- Rollback-ferli skjalfest og prófað (sjá §11.3) (**Verkkaupi**)
- Handvirkar samþykktir skilgreindar fyrir Production (sjá §11.1) (**Verkkaupi**)

Rekstrarviðbrögð og atvik

Viðbragðsferlar

- Viðbragðsferlar skilgreindir fyrir hvert alvarleikastig (sjá §10.1) (**Verkkaupi**)
- Úthringiferli (on-call, escalation) skilgreint (**Verkkaupi**)
- Tengiliðalisti uppfærður (**Verkkaupi**)

Atvik

- Atvikaskráning og eftirfylgni skilgreind (sjá §10.3) (**Verkkaupi**)
- Post-mortem ferli skilgreint (sjá §10.5) (**Verkkaupi**)
- Tilkynningarskyldur skjalfestar (sjá §10.2) (**Verkkaupi**)

Sambætting við ytri þjónustur

- Tengingar við ytri kerfi vaktaðar og prófaðar (**Verkkaupi**)
- SLA og viðbragðstímar ytri þjónustu skjalfestir (**Verkkaupi**)

Gagnagrunnar og afritun

- Afritun skilgreind og prófuð samkvæmt §8.5 (**Verkkaupi**)
- Endurheimtarferli (restore) skjalfest og prófað samkvæmt §8.6 (**Verkkaupi**)
- Backward-compatibility kröfur staðfestar við gagnagrunnsbreytingar (**Verkkaupi**)

Stöðusíður og samskipti

- Lausn tengd stöðusíðu (**Verkkaupi**)
- Samskiptaferlar við notendur skilgreindir við truflanir (sjá §10.4) (**Verkkaupi**)

Langtímarekstur og samningar

- SLA þjónustustig skilgreind (sjá §8.1) (**Verkkaupi**)
- Uppitímakröfur og viðurlög skjalfest (**Verkkaupi**)
- Endurskoðun rekstrarferla skipulögð reglulega (**Verkkaupi**)
- Endurskoðun aðgangsheimilda skipulögð (sjá §6.1) (**Verkkaupi**)

Viðauki 5: Ábyrgðarskipting (RASCI)

Auk þeirra aðila sem skilgreindir eru í RASCI-töflu þessari starfa eftirfarandi lykilhlutverk í stjórnskipan Stafrænnar heilsu og bera ábyrgð á tæknilegri og klíniskri samhæfingu lausna. Hlutverkin eru lágmarksviðmið; einstök verkefni geta haft fleiri hlutverk, og sami einstaklingur getur gegnt fleiri en einu hlutverki þegar umfang verkefnis kallar á það. Skipan hlutverka skal skjalfest í verkefnaskjöllum.

Hlutverk	Ábyrgð
Tæknilegur verkefnastjóri	Tæknileg heildarmynd lausnar, samræmi við tæknistefnu, val á tækni og arkitektúr, tæknileg samþætting við önnur kerfi og tæknileg áhættustýring.
Klínískur verkefnastjóri	Að lausnir styðji klínískt verklag og ferla, að notkun og miðlun gagna sé klínískt rétt og samþykkt, og að tenging milli klínískra þarfa og tæknilegrar útfærslu sé tryggð.

Þessi hlutverk eru viðbót við þá aðila sem skilgreindir eru í næsta hluta (Aðilar) og taka þátt í RASCI-töflu hér að neðan eftir því sem við á; tæknilegur verkefnastjóri svarar að jafnaði til hlutverka tæknilegra ábyrgðaraðila (TÁ) og verkefnastjóra (VS), eftir umfangi verkefnis.

Aðilar

Skammstöfun	Aðili
TÁ	Tæknilegir ábyrgðaraðilar verkkaupa
RT	Rekstrarteymi verkkaupa
ÖS	Öryggisstjóri verkkaupa
VS	Verkefnastjóri verkkaupa
ÞA	Þjónustuaðili / hýsingaraðili
VT	Verktaki (verksali)
ST	Stjórnendur verkkaupa
TVS	Tæknilegur verkefnastjóri
KVS	Klínískur verkefnastjóri

Lykill

Hlutverk	Lýsing
R (Responsible)	Framkvæmir verkþáttinn
A (Accountable)	Ber endanlega ábyrgð og tekur ákvörðun
S (Supportive)	Styður framkvæmd
C (Consulted)	Ráðfærður áður en ákvörðun er tekin
I (Informed)	Upplýstur um stöðu og niðurstöður
—	Ekki hlutdeild í verkþætti

RASCI-tafla

Taflan sýnir hvern verkþátt í öðrum dálki og alla aðila sem koma að rekstri í efstu röð. Í hverjum reit stendur bókstafur sem segir til um hlutverk viðkomandi aðila í þeim verkþætti:

Verkþáttur	TÁ	RT	ÖS	VS	ÞA	VT	ST
Vöktun og viðvaranir							
Dagleg vöktun og viðvaranir	C	R	I	I	S	—	I

Skilgreining viðvörðunarþröskulda	A	R	C	I	S	—	I
Viðhald mælaborða	C	R	—	I	S	—	—
Viðbrögð við atvikum							
Viðbrögð við Critical atvikum	A	R	C	I	S	S	I
Viðbrögð við Medium atvikum	C	R	I	I	S	—	—
Viðbrögð við mildum atvikum	—	R	—	I	S	—	—
Post-mortem og eftirfylgni	A	R	C	I	S	C	I
Bakvaktir							
Bakvakt Kubernetes	C	S	—	I	R	—	—
Bakvakt gagnagrunnar	C	S	—	I	R	—	—
Bakvaktarhugbúnaður (application)	A	R	—	I	S	S	—
Atvikaskráning							
Skráning atvika	C	R	I	I	S	—	—
Tilkynning til eftirlitsaðila (öryggisbrestur)	C	S	A	I	—	—	I
Uppfærsla stöðusíðu	I	R	—	I	S	—	I
Útgáfur							
Samþykkja útgáfu í PreProduction	A	S	—	I	S	R	—
Samþykkja útgáfu í Production	A	S	—	I	—	—	I
Framkvæma útgáfu (CI/CD)	S	R	—	I	S	—	—
Gagnagrunnsbreytingar	A	S	—	I	R	C	—
Rollback-ákvörðun	A	S	C	I	S	C	I
Neyðarbreytingar							
Samþykkt neyðarbreytingar	A	S	C	I	S	C	I
Framkvæmd neyðarbreytingar	S	R	I	I	S	S	I
Skjalfesting eftir neyðarbreytingu	C	R	I	I	S	C	—
Aðgangsstýring							
Veiting aðgangs starfsmanna	C	R	A	I	—	—	—
Veiting aðgangs verktaka	C	R	A	I	—	—	—
Reglubundin endurskoðun aðganga	C	S	A	I	—	—	I
Afturköllun aðgangs við starfslok/samningslok	C	R	A	I	—	—	—
Afritun og endurheimt							
Afritun gagnagrunna	C	S	—	I	R	—	—
Prófun á endurheimt (restore)	A	S	—	I	R	—	—

Endurheimt við atvik	A	R	C	I	S	—	I
Skjölun							
Viðhald rekstrarskjalanna	A	R	—	I	S	—	—
Viðhald innviðateikninga	C	R	—	I	S	—	—
Endurskoðun rekstrarhandbókar (árleg)	A	S	C	C	C	—	I

Dæmi: Ef röðin „Samþykkja útgáfu í Production“ sýnir $TA = A$, $RT = S$, $VS = I$ þýðir það að tæknilegir ábyrgðaraðilar bera endanlega ábyrgð á samþykktinni, rekstrarteymi styður framkvæmdina og verkefnastjóri er upplýstur um niðurstöðuna.

Athugasemdir

- Þessi tafla er leiðbeinandi viðmið. Nákvæm RASCI-skipting getur verið mismunandi eftir verkefnum og samningum.
- Verkaupi ber ábyrgð á að endurskoða og uppfæra RASCI-töflu eftir þörfum, sérstaklega við breytingar á samningum eða skipulagi.
- Einn aðili getur haft mismunandi hlutverk eftir verkþáttum.
- Fyrir hvern verkþátt skal nákvæmlega einn aðili vera merktur A (Accountable).

