Lisa 1

TEHIK INFOSÜSTEEMIDE TALITLUSPIDEVUSE HALDAMISE KORD

1. Üldsätted

1.1. TEHIK infosüsteemide talitluspidevuse haldamise kord (edaspidi kord) sätestab Tervise ja Heaolu Infosüsteemide Keskuse (edaspidi TEHIK) hallatavate infosüsteemide talitluspidevuse halduse reeglid.

1.2. Korra eesmärk on tagada infosüsteemide taastamiseks vajalike varukoopiate ja taasteplaanide olemasolu ning vajadusel infosüsteemide õigeaegne töövõime taastamine.

1.3. Korra omanik on TEHIK baasteenuste osakonna juht.

2. Seotud dokumendid

2.1. Mõisted (TEHIK Atlassian keskkonnas asuv jooksvalt täienev dokument)

2.2. Intsidentide haldamise kord (TEHIK Delta)

2.3. Hädaolukorra lahendamise plaan HOLP (TEHIK Delta)

3. Mõisted

3.1. **Administraator** – käesoleva korra mõistes TEHIK töötaja, kelle kohustuseks on infosüsteemi komponentide haldamine.

3.2. **Andmekadu** – andmete soovimatu kustutuse või ebakorrektseks muutumise tagajärg.

3.3. **Diferentsiaalne varundus** – varunduse tüüp, varundus, mille puhul kopeeritakse ainult pärast viimast täielikku varundust muutunud andmed .

3.4. **Eriolukord -** planeerimata katkestus katastroofi olukorras ehk ootamatu sündmus, mille korral on infosüsteemi(de) toimimiseks vajalik füüsiline IT-infrastruktuur vähemalt ühes lokatsioonis hävinud või kahjustunud ja see katkestab infosüsteemi(de) normaalse talitluse ning selle taastamiseks on vajalik rakendada taasteplaani.

3.5. **Infosüsteem** – TEHIK hallatava riistvara, tarkvararakenduste ja nende abil töödeldavate andmete kogum.

3.6. **Infosüsteemide haldussüsteem** – eraldi infosüsteem, mille abil jälgitakse ja hallatakse infosüsteemide tööd. Infosüsteemide haldussüsteemide mittetöötamise korral on raskendatud või seiskub probleemide avastamine ning lahendamine, mis omakorda võib kaasa tuua kriitiliste süsteemide töö seiskumise.

3.7. **Infovara omanik** – avaliku teabe seaduse mõistes vastutav töötleja või tema poolt määratud struktuuriüksus juhi isikus ning muudel juhtudel asutuse juhi poolt määratud struktuuriüksus juhi isikus.

3.8. **Inkrementaalne varundus** – varunduse tüüp. Varundus, mille puhul kopeeritakse ainult pärast eelmist varundust muutunud andmed.

3.9. **Intsident** - ootamatu rike, mis ei ole normaalse/standardse teenuse osa, mis põhjustab või võib põhjustada infosüsteemi planeerimata katkestuse või teenuse kvaliteedi olulise languse.

3.10. **Infosüsteemide talitluspidevuse haldus** - protsess, mis vastutab infosüsteeme tõsiselt mõjutada võivate riskide haldamise eest. Protsess kindlustab riskide vähendamise ja infosüsteemide taastamise planeerimise abil, et infosüsteemi käideldavustingimused oleks tagatud.

3.11. **Kriitilisuse klass** - infosüsteemi taastamise maksimaalne ajakulu ning prioriteet, mille järjekorras eriolukorra puhul infosüsteeme taastatakse. IT-teenuse kriitilisuse klassid on sätestatud teenustaseme lepingutes mis on sõlmitud asutustega kellele Keskus IT-teenust osutab. Kui teenusele ei ole kriitilisuse klassi määratud loetakse, et teenuse taasteaeg on määratlemata.

3.12. **Oluline infosüsteemi muudatus** – infosüsteemi komponentides tehtavad muudatused, ümberkorraldused ja täiendused, mis muudavad süsteemi toimimise loogikat ja võivad mõjutada süsteemi käideldavust ja andmeterviklust.

3.13. **Planeerimata katkestus** – infosüsteemi tööajal toimuv mitteplaanipärane infosüsteemi või selle funktsionaalsuse katkestus (sh kolmandate osapoolte põhjustatud) või häire nende töös.

3.14. **Planeerimata katkestuse lubatud maksimaalne aeg** – aeg, mis võib kuluda planeerimata katkestuse kõrvaldamisele koos taasteplaani järgi taastamiseks kuluva ajaga (ei kehti eriolukorras).

3.15. **Põhiinfosüsteem** – kriitiline infosüsteem mida kasutatakse asutuse põhifunktsioonide teostamiseks ja teenuste pakkumiseks välistele osapooltele.

3.16. **Seire** – konfiguratsioonielemendi, infosüsteemi või protsessi korduv jälgimine sündmuste avastamiseks ja kindlustamaks, et seiratava objekti jooksev staatus oleks teada.

3.17. **Taaste (*recovery*)** – pärast intsidenti infosüsteemi komponentide taastamine ja taas ühendamine infosüsteemi ehk tagasiviimine olekusse, milles ta saab täita nõutavaid ülesandeid.

3.18. **Taasteaeg** – lubatav maksimaalne ajaperiood, mille jooksul tuleb infosüsteem, mille töövõime on osaliselt või täielikult kadunud, taasteplaani järgi taastada nõutud funktsionaalsuse ja jõudluse tasemele.

3.19. **Taasteaeg eriolukorras** – kokku lepitud maksimaalne lubatav ajaperiood eriolukorras, mille jooksul tuleb infosüsteemi IT-infrastruktuur, taastada kokkulepitud funktsionaalsuse ja jõudluse tasemele.

3.20. **Taasteplaan** – dokumenteeritud protseduur, mis kirjeldab infosüsteemi komponentide taastamise ja taas ühendamise infosüsteemi ning määrab vastutavad isikud.

3.21. **Teenusehaldur** –tagab igapäevaselt infosüsteemi sisulise toimimise ja arendab infosüsteemi koostöös vastutava töötleja ja peakasutajaga. Tunneb infosüsteemi ärilist sisu

ja tehnilist lahendust, oskab analüüsida (kaasates teisi osapooli) infosüsteemi muutmisega kaasnevat mõju süsteemile ja sellega seotud teenustele. Vastutab infosüsteemi haldusega/hooldusega seotud lepingute (sh SLA) ja vajalike litsentside olemasolu ja uuendamise eest, samuti infosüsteemi korrektse dokumenteerimise ja nõutud aruandluse eest.

3.22. **Tugiinfosüsteem** – infosüsteemid, mida kasutatakse organisatsioonisiseselt äriprotsesside toetamiseks.

3.23. **Täielik varundus** – varunduse tüüp, infosüsteemi kõigi andmete ja/või kogu tarkvara täielik varukopeerimine.

3.24. **Varundamine** – andmetest varukoopiate tegemine hilisemaks taastamiseks juhul, kui originaalandmed peaksid hävinema või rikutud saama.

3.25. **Varundusmeedia** – andmekandja, millele salvestatakse varundamisele kuuluvad andmed.

3.26. **Varukoopia** – süsteemi mõjutavate komponentide (rakendusandmed, süsteemiandmed, tarkvara, logiandmed) koopia, mis on tehtud teatud hetke seisuga ning mis pärast intsidenti võimaldab süsteemi ennistamist.

3.27. **Varunduslahendus** – tarkvara ja meedia lahendused, mida kasutatakse infosüsteemide varundamiseks.

4. Talituspidevuse tagamiseks kasutatavad meetodid ja vahendid

4.1. Infosüsteemide talituspidevuse kindlustamiseks tehakse varukoopiaid vastavalt andmevarunduse korrale ja varundusplaanidele.

4.2. Infosüsteemide taastamiseks kasutatavad meetodid ja vahendid määratletakse taasteplaanides.

4.3. Infosüsteemi komponentide dubleerimine.

4.3.1. Infosüsteemi serverid kriitilisuse klassiga I dubleeritakse.

4.3.2. Infosüsteemi sidevõrgud kriitilisuse klassiga „tegevuskriitiline" dubleeritakse.

4.3.3. Infosüsteemide komponentide dubleerimist teostab süsteemiadministraator.

4.4. Spetsiaalsed tööjaamad ja seadmed, mida kasutatakse infosüsteemi komponentide haldamiseks, dubleeritakse.

4.5. Tarkvarale ja seadmetele, mis kuuluvad kriitilisuse klassiga „tegevuskriitiline" infosüsteemide komponentide hulka, sõlmitakse tootetoe lepingud. Tootetoe lepingute sõlmimise eest vastutab baasteenuste osakonna juhataja.

4.6. Laovaru kasutatakse tüüpkonfiguratsiooniga hõlpsalt installeeritavate infosüsteemi riistavara komponentide korral, mis kuuluvad kriitilisuse klassi „tegevuskriitiline", „kriitiline" ning mille käideldavusklass on K3 või kõrgem, mille korral dubleerimine ja/või tootetoe lepingute sõlmimine ei ole võimalik või otstarbekas.

4.7. Kõigi infosüsteemi riistvara komponentide taastamiseks, millele ei rakendata dubleerimist, tootetoe lepingu sõlmimist või laovaru soetamist, teostatakse hange vajaduse tekkimisel.

5. Andmevarunduse kord

5.1. Andmekao vältimiseks ja talituspidevuse tagamiseks tuleb kõiki infosüsteeme vastavalt varundusplaanidele regulaarselt varundada.

5.2. TEHIK poolt hallatavate infosüsteemide varundusplaanide koostamise korraldamise, halduse ja regulaarse testimise eest vastutab infosüsteemi teenusehaldur või seda rolli täitev isik.

5.3. Põhiinfosüsteemide varundusplaanide koostamise, toimimise ja halduse eest vastutavad isikud (esmane, asendaja) määrab baasteenuste osakonna juhataja.

5.4. Varundust peab teostama infosüsteemist eraldi asuva varunduslahenduse pinnale.

5.5. Varundatud koopiad peavad olema krüpteeritud.

5.6. Varukoopiate tegemise aeg ja meetod peab tagama infosüsteemile määratud taasteaja, käideldavusnõuete ja andmetervikluse nõuete täitmise ja olema kooskõlas süsteemi või teenuslepingu juurde kuuluvate käideldavustingimuste nõuetega.

5.7. Minimaalselt varundatakse kõiki infosüsteeme vähemalt üks kord ööpäevas diferentsiaalse varunduse koopiana ja üks kord nädalas täieliku varunduse koopiana. Säilitada tuleb vähemalt kolme viimast täieliku varunduse koopiat.

5.8. Varundamisele kuuluvate andmete konfidentsiaalsus- ja terviklusnõudeid tuleb kohaldada ka varundusmeediale.

5.9. Kui varundatavate andmete töötlemisel tuleb kinni pidada kustutustähtaegadest (nt isikuandmete puhul), tuleb varundatud andmed kustutada ka varundusmeedialt.

6. Varundusplaan

6.1. Varundusplaanid asuvad ja neid hallatakse TEHIK baasteenuste osakonna Atlassian keskkonnas.

6.2. Varundusplaanide koopiad säilitatakse välisel andmekandjal PDF failiformaadis koos taasteplaanidega TEHIK Infoturbeosakonna (edaspidi ITO) seifis.

6.2.1. Varundusplaanide kopeerimine välisele andmekandjale ja deponeerimine ITO seifi toimub vähemalt kaks korda aastas ja selle eest vastutab TEHIK Baasteenuste osakond.

6.3. Varundusplaanid tuleb teenusehalduri või seda rolli täitva isiku poolt üle vaadata kaks korda aastas (hõlmab summaarselt ka p6.4 nõuet) ja testida koos taasteplaanide testiga kord aastas.

6.4. Varundusplaanid tuleb üle vaadata ja testida ka pärast infosüsteemi või mõne infosüsteemi toimimiseks vajalike süsteemide olulisi tarkvaralisi või riistavaralisi muudatusi või peale mõjuga küberründe toimumist.

6.5. Varundusplaan koostatakse Varustusplaani vormil vastavalt lisale 1.1 ja selles kirjeldatakse:

6.5.1. infosüsteemi/teenuse nimi;

6.5.2. varundusplaani koostamise aeg;

6.5.3. infosüsteemi/teenuse kriitilisuse klass ja lubatud andmekadu ajas;

6.5.4. andmete varundamise aeg, sagedus ja tüüp;

6.5.5. varundatavate andmete loend (seade, server, teenus, andmebaasid, failid jms) ja eeldatav maht;

6.5.6. varukoopia säilitamise aeg, säilitatavate põlvkondade arv, arhiveerimise eesmärgil säilitatavad varundused jmt;

6.5.7. andmete varundamise eest vastutav administraator. Vajalik, kui varunduslahendus on erinev kesksest põhiinfosüsteemi varundusest;

6.5.8. varundusplaani ülevaatuse/uuendamise aeg.

7. Varukoopiate säilitamine ja transport

7.1. Infosüsteemide varukoopiad säilitatakse varundusmeedial infosüsteemist eraldi asuvas lokatsioonis.

7.2. Juurdepääs varukoopiale ja/või varundusmeediale on lubatud ainult infosüsteemi rakendusadministraatoritele, Baasteenuste osakonna ja ITO töötajatele.

7.3. Pikaajalisele säilitamisele kuuluvad varukoopiad tuleb säilitada koos taasteplaaniga, Säilitamistingimused määratakse varundusplaanis.

7.4. Varundusandmete transpordil üle andmesidekanalite peab kasutama ainult turvalisi tehnoloogiaid ja transporditavad andmed peavad olema krüpteeritud.

7.5. Füüsilise varukoopia transportimine dokumenteeritakse varundusmeedia registris TEHIK Baasteenuste Atlassian keskkonnas.

7.6. Varukoopia transpordiviis kooskõlastatakse infoturbeosakonnaga. Varundusmeedia peab säilitamisel või transpordil olema kaitstud käideldavuse ja tervikluse rikkumise ning volitamata juurdepääsu eest.

7.7. Transporditavad andmed peavad krüpteeritud andmekandjal olema kogu teekonna ja hoidmise vältel pakendatud turvapakenditesse, mille avamistest jääb jälg.

7.8. Varukoopia, mis on mõeldud andmete transportimiseks ja/või kellelegi üleandmiseks ning mille andmeid ei ole mõnel teisel andmekandjal, tuleb eelnevalt varundada.

7.9. Varukoopia üleandmine transpordiks kolmandale isikule fikseeritakse dokumendihaldussüsteemis üleandmise akti või saatekirjaga, mis sisaldab saatjat, vastuvõtjat, andmekandja liiki ja identifitseerimis tunnuseid, saatmise või üleandmise kuupäeva, osapoolte allkirju ning vajadusel andmete säilitamise või hävitamise tingimusi. Akt kooskõlastatakse infoturbeosakonnaga.

7.10. Varundusest kõrvaldatud varundusmeedia hävitamine kooskõlastatakse infoturbeosakonnaga, hävitamise korraldab baasinfrastruktuuri tiim .

8. Taasteplaanide üldreeglid

8.1. TEHIK poolt hallatavate infosüsteemide taasteplaanide koostamise korraldamise, haldamise ja regulaarse test taaste läbiviimise eest vastutab infosüsteemi teenusehaldur või seda rolli täitev isik.

8.2. Põhiinfosüsteemide taasteplaanide koostamise ja halduse eest vastutavad isikud (esmane, asendaja) määrab TEHIK Baasteenuste osakonna juhataja.

8.3. Taasteplaanid asuvad ja neid hallatakse TEHIK Baasteenuste osakonna Atlassian keskkonnas.

8.4. Taasteplaanid säilitatakse koopiana välisel andmekandjal PDF failiformaadis koos infosüsteemi varundusplaaniga ning kaitstult volitamata juurdepääsu eest ITO seifis.

8.4.1. Taasteplaanide kopeerimine välisele andmekandjale ja deponeerimine ITO seifi toimub vähemalt kaks korda aastas ja selle eest vastutab TEHIK Baasteenuste osakond.

8.4.2. Põhiinfosüsteemide taasteplaanid säilitatakse lisaks elektroonilisele koopiale ITO seifis ka paberkandjal.

8.5. Taasteplaanid koostatakse:

8.5.1. Vähemalt kõigile põhiinfosüsteemidele ja kriitiliste teenuste infosüsteemidele.

8.5.2. Kõigile uutele infosüsteemidele, mis lisanduvad toodangukeskkonda (tulenevalt standardsetest käideldavusnõuetest, mis määravad infosüsteemidele maksimaalse planeerimata katkestuse aja).

8.5.3. Enne infosüsteemi oluliste muudatuste tegemist (juhul kui taasteplaan puudub) tagamaks süsteemi taaste peale muudatuste rakendamise ebaõnnestumist.

8.5.4. Serveriruumidele ja andmekeskustele juhuks , kui mõni nimetatud ruumidest või ruumi toetav infrastruktuur hävib või seda ei saa teatud aja jooksul kasutada (plaan põhiinfosüsteemi taasteks teises lokatsioonis).

8.5.4.1. TEHIK poolt renditud serveriruumide ja andmekeskuste toetava infrastruktuuri taasteplaanide eest on vastutav lepinguline rendile andja.

8.6. Taasteplaanide koostamisel tuleb aluseks võtta Taasteplaani vorm, mis koostatakse vastavalt lisale 1.2.

8.7. Taasteplaanide tegemisel tuleb arvestada, et taastamise hetkel ei pruugi kõik infosüsteemi komponendid olla kättesaadavad ja taastaja on infosüsteemi põhiadministraatorist erinev isik. See tähendab, et taastamiseks vajalikust standardtarkvarast, konfiguratsioonifailidest, infosüsteemi tarkvarast, installeerimisjuhenditest ja muudest taastamiseks vajalikest rakendustest ja dokumentidest peavad eksisteerima varukoopiad, mis asuvad taastatavast süsteemist eraldi asukohas ja on vajadusel kättesaadavad.

8.8. Taasteplaanid peavad kindlustama infosüsteemide taaste ettenähtud taasteaja jooksul ka juhul, kui samaaegselt tuleb taastada mitu või kõik infosüsteemi osad või erineva kriitilisuse tasemega infosüsteeme.

8.9. Taasteplaani järgi taastamine käivitub hiljemalt siis, kui ühe planeerimata katkestuse maksimaalse kestvuse ajast on ära kulunud intsidendi kõrvaldamiseks lubatud aeg.

8.10. Taasteplaani järgi taastamiseks kuluv aeg ja muud tegevused ei tohi ületada ühe planeerimata katkestuse maksimaalset kestvust (v.a eriolukord).

8.11. Eriolukorra puhul käivitub taasteplaan koheselt.

8.12. Infosüsteemidele juurdepääsu tagamiseks peavad kõigi süsteemide administraatorite paroolid olema hoiustatud paroolihoidlas ja koopia deponeeritud ITO seifi väljaprindina. Paroolihoidlast koopia tegemise ja seifi deponeerimise eest vastutab ITO.

9. Taasteplaanide haldamine ja testimine

9.1. Taasteplaani koostamise ja halduse eest vastutav isik peab tagama plaani kasutatavuse ja ajakohasuse ning plaani ülevaatamise vähemalt kaks korda aastas (hõlmab summaarselt ka p9.2 nõuet) ja testimise vähemalt kord aastas.

9.2. Taasteplaanid vaadatakse üle ja testitakse ka pärast infosüsteemi või mõne infosüsteemi toimimiseks vajalike süsteemide olulisi tarkvaralisi või riistavaralisi muudatusi või peale *intsidendi (sh küberründe)* tekkimist, mille põhjuseks oli taasteplaani puudulikkus või taasteplaani mitte järgimine.

9.3. Test taastamist tuleb teostada testkeskkonnas, kus süsteem taastatakse nullseisundist normaaltalituse tasemele.

9.4. Taasteplaani testimine peab sisaldama tarkvara ja andmete varukoopiatest taaste testimist, kui varundus ja taasteplaanides on varukoopiad ette nähtud.

9.5. Test taastamist peab teostama infosüsteemi põhiadministraatorist erinev administraatori kvalifikatsiooniga töötaja.

9.6. Taasteplaani testimise, mille läbiviimine võib mõjutada tegevuskriitilise infosüsteemi tööd, aja ja ulatuse määrab Baasteenuste osakonna juhataja.

10. Taasteplaanis käsitletav teave

10.1. Taasteplaan peab sisaldama minimaalselt:

10.1.1. süsteemi lubatud andmekadu ajas;

10.1.2. intsidendi kõrvaldamiseks lubatud maksimaalne ajakulu;

10.1.3. süsteemi taastamiseks kuluvat ja nõutud aega, taasteaeg;

10.1.4. taasteks vajamineva riistvara miinimum- ja ideaalkonfiguratsiooni.;

10.1.5. riistvaraliste komponentide paigaldamiseks vajalik teave (nt serveri nimi, kaabeldused, võrgupesa nr jms);

10.1.6. tarkvaraliste komponentide spetsifikatsioone (sh ka versioonid);

10.1.7. võrguparameetreid (nt IP-aadress, VLAN'i nr, lubatud pordid jms);

10.1.8. süsteemi administraatoriparoolide asukohta;

10.1.9. kasutatava riistvara garantii-, asendus- ja tugitingimusi, alternatiivvariante taasteks vajaliku riistvara leidmiseks;

10.1.10. taasteks vajamineva tarkvara versioone ja nende varukoopiate asukohta;

10.1.11. andmete varukoopiate asukohta ja varundusmeedia tähist;

10.1.12. taastamiseks vajaminevate konfiguratsioonifailide, krüptovõtmete ja juhendite (installeerimisjuhendid, administreerimisjuhendid, liideste kirjeldused jms) asukohta;

10.1.13. taastamise protseduurid kujul, et taastamine on võimalik ka süsteemi detailselt mittetundva administraatori poolt;

10.1.14. taastamisega seotud isikute kontaktandmed;

10.1.15. taastetoimingute viimase testimise kuupäeva.

10.2. Kui taasteplaan näeb ette uue riist- või tarkvara hankimist, peab plaan sisaldama asendushanke toiminguid, st kirjeldust (ka tehnilist), kuidas võimalikult kiiresti riist- ja/või tarkavara hankimine läbi viia ning kui palju see eeldatavalt aega ja rahalisi ressursse võtab.

10.3. Taasteplaani detailsus peab olema piisav, et süsteemiadministraatori kvalifikatsiooniga isik on suuteline taasteplaani järgi infosüsteemi komponente taastama.

10.4. Kolmandatele osapooltele, v.a seadusega määratud asutustele, võimaldatakse vajadusel juurdepääs taasteplaanile üksnes konfidentsiaalsusleppe olemasolul.

11. Taasteaegade määramine

11.1. Infosüsteemi taasteaegadele esitatavad nõuded kehtestab infovara omanik. Infosüsteemi käideldavusele esitatavad nõuded kirjeldatakse infosüsteemi käideldavustingimustes.

11.2. Infosüsteemi taasteaegade vastavuse eest käideldavustingimustele vastutab teenusehaldur või seda rolli täitev isik.

11.3. Kriitilisuse klass väljendab infosüsteemi taastamise prioriteeti, mis järjekorras eriolukorras infosüsteeme taastatakse. Lähtuvalt taasteaegadest jaotatakse infosüsteemi osad järgmistesse kriitilisuse klassidesse:

11.3.1. **I (tegevuskriitiline)** - taasteaeg kuni 3 ööpäeva (72h).

11.3.2. **II (oluline)** - taasteaeg kuni 7 ööpäeva (168h).

11.3.3. **III (madal)** - taasteaeg määratlemata.

12. Taaste prioriteedid

12.1. Infosüsteemide komponendid taastatakse rangelt kriitilisuse klasside alusel alustades klassist I, seejärel klass II ja klass III.

12.2. Iga kriitilisuse klassi piires toimub taastamine alljärgnevas järjestuses:

12.2.1. põhiinfosüsteem;

12.2.2. infosüsteemi haldussüsteem (kasutajatoe tarkvara, serverite seire tarkvara);

12.2.3. tugiinfosüsteem;

12.2.4. arenduse- ja testimise infosüsteem.

12.3. Taaste prioriteete on lubatud muuta:

12.3.1. kui madalama prioriteediga infosüsteemi taastamine enne või koos kõrgema prioriteediga infosüsteemiga ei too kaasa taasteressursside konflikti.

12.3.2. baasteenuste osakonna juhataja otsusega.

Lisa 1.1

Varundusplaani vorm

Asub https://spot.tehik.ee/display/INFRA/Varundusplaanid „LISA UUS VARUNDUSPLAAN"

Infosüsteemi/teenuse .....varundusplaan

Varundusplaani koostamise kuupäev: dd.mm.yyyy

Infosüsteemi/teenuse kriitilisuse klass ja lubatud andmekadu ajas:

klass I-III;

andmekadu oh oomin

Varunduse kirjeldus

Kuidas ja millega tehakse:

Kus, kuidas säilitatakse:

Andmete varundamise sagedus, aeg, tüüp ja säilitusaeg

Sagedus	Aeg	Tüüp	Säilitamisaeg

Varundatavate andmete loend (seade, server, teenus, andmebaasid, failid jms) ja eeldatav maht.

Seade, teenus jne.	Kirjeldus	Maht

Andmete varundamise eest vastutav administraator, Vajalik, kui varunduslahendus on erinev kesksest põhiinfosüsteemi varundusest

esmane:

asendaja:

Varundusplaani viimane ülevaatus dd.mm.yyyy

Varundusplaani testimine:

Näiteks: Koos taasteplaani testiga + sagedus.

Lisa 1.2

Taasteplaani vorm

Asub https://spot.tehik.ee/display/INFRA/Taasteplaanid **„LISA UUS TAASTEPLAAN"**

Taasteplaan

Käesoleva dokumendi eesmärk on tagada infosüsteemi _____ taastamine vastavalt kokkulepitud nõuetele.

Teenuse/funktsiooni nimi	"Infosüsteemi,teenuse" taasteplaan
Teenuse juht	**@Nimi,** Tel. xxx xxxx
Teenuse haldajad	esmane **@Nimi,** Tel. xxx xxxx teine **@Nimi,** Tel. xxx xxxx
Süsteemi lubatud andmekadu ajas	max lubatud andmekadu ajas RPO, kui on sõlmitud SLA või OLA, siis vastavalt sellele. **o h oomin**
Intsidendi kõrvaldamiseks lubatud maksimaalne ajakulu	intsidendi kõrvaldamiseks lubatud maksimaalne ajakulu ehk **aeg, mille lõppedes alustatakse taastamist taasteplaani järgi**. **o h oomin**
Süsteemi taasteaeg	**o h oomin**
Planeerimata katkestuse lubatud maksimaalne aeg, SLA max katkestus	Teenustasemeleppes määratud ühekordse **planeerimata katkestuse maksimaalne kestvus.** **o h oomin**
Taasteplaani ülevaatuse sagedus ja viimane ülevaatuse kuupäev	Sagedus, kaks korda aastas **mm, mm** Taasteplaan kontrollitud, kuupäev **dd.mm.yyyy**
Taasteplaani testimine ja viimase testi läbiviimise aeg	Taasteplaani testitakse vähemalt kord aastas **mm.yyyy,** Viimati testitud, kuupäev **dd.mm.yyyy** ja testi läbiviija **@Nimi**

Taasteplaani kinnitamine	Ametinimetus, **@Nimi**

Taastestrateegia

Taastemeeskond

Järgnevalt loetletud töötajad vastutavad taasteprotseduuride täitmise eest või tagavad protseduuride täitmise ning esinenud probleemide ülesmärkimise.

Ees- ja perekonnanimi	Ametikoht	Kontakteerumisviis

TEHIK sisemiste ja väliste kontaktide nimekiri

Ees- ja perekonnanimi	Organisatsioon ja roll	Ametikoht	Kontakt

Seosed teiste süsteemidega

Süsteemide omavahelised sõltuvused tuleb kirjeldada alljärgnevalt olulisuse järjekorras, et käesoleva taasteplaaniga seotud teisi taasteplaane vajadusel kasutada.

Süsteem	Viide dokumendile	Kontaktisik
Kirjeldus, nimi		

Seosed teiste taasteplaanidega

Käesolevas punktis kirjeldatakse seosed teiste TEHIK hallatavate taasteplaanidega ning nende aktiveerimine.

Teised taasteplaanid	Seos
Kirjeldus, nimi	

Varundusteave

Varundusega seotud teave kirjeldatakse teenuse varundusplaanis (märkida viide).

Süsteemi varundusplaan	Varunduse asukoht
Kirjeldus, nimi	

Infosüsteemi tehniline info

Riistvaraliste komponentide spetsifikatsioon ja riistvaraliste komponentide paigaldamiseks vajalik teave

Füüsilise riistvara puhul täita ainult vastava teenuse või infosüsteemi poolt otseselt kasutatud ja/või hallatavad seadmed. Näiteks Kubernetes, VMware, varundus, andmebaasid, võrgud. Kasutatava riistvara puhul näidata garantii-, asendus- ja tugitingimusi, alternatiivvariante taasteks vajaliku riistvara leidmiseks(hanked).

Komponentide spetsifikatsiooni peab muutma vajadusel vastavaks kasutusel olevate seadmetega.

1-Komponentide spetsifikatsioon

Info CMDB's	<link>
Server/vm	
CPU(vm reservatsioon)	
RAM(vm reservatsioon)	
FC HBA	
NIC	
HDD	
Kaughaldus	

Komponentide paigaldamiseks vajalik teave

Nimed võrgus	dba.asutus.sise, dbb.asutus.sise, dbc.asutus.sise
Füüsiline paiknemine	AK, kapp,

Võrgupesad	bay1-port1, bay2-port1,

2-Kubernetes

Info CMDB's	<link>
Klaster	
Projekt	
Nimeruumid	
Kubernetes server version	
Kubernetes client version	
Nimeruumide RAM quota	
Nimeruumide CPU limits	
Operaatorid	
GIT repo helm-chartidele	

Riistvaraliste komponentide paigaldamiseks vajalik teave

Nimed võrgus	dba.asutus.sise, dbb.asutus.sise, dbc.asutus.sise
Füüsiline paiknemine	AK, kapp,
Võrgupesad	DB bay1-port1, bay2-port1,

3-Riistvaraliste komponentide spetsifikatsioon

Info CMDB's	<link>
Seade	

CPU	
RAM	
FC HBA	
NIC	
HDD	
Kaughaldus	

Riistvaraliste komponentide paigaldamiseks vajalik teave

Nimed võrgus	dba.asutus.sise, dbb.asutus.sise, dbc.asutus.sise
Füüsiline paiknemine	AK, kapp,
Võrgupesad	DB bay1-port1, bay2-port1,

Nõuded riistvaralistele asendusressurssidele

Minimaalsed nõuded komponentidele, st seadmetele ja tarkvarale

Server	
CPU	
RAM	
FC HBA	
NIC	
HDD	
Kaughaldus	

Nõuded kohustuslikule laovarule, mida ei saa katta olemasolevate universaalsete asendusressurssidega.

Seade	

Nõuded kohustuslikule laovarule, mida ei saa katta olemasolevate universaalsete asendusressurssidega.

Seade	

Tarkvaraliste komponentide spetsifikatsioon

Operatsiooni süsteem, versioon	Windows Server 2022 build 20348.3692 , OracleLinux-R9-U5
Rakendustarkvarad, versioon	Oracle GRID infrastructure 11.2.3.4.6
Eeldus-tarkvarad, versioon	Oracle Database RAC 11.2.3.4.6

Võrguparameetrid

Serverite ifconfig väljavõte normaalolukorras ja kasutatavad VLAN-d

- etho on trunc port, operatsioonisüsteemist vlan123
- eth1 on vlan124
- 192.168.1.1 dba.asutus.sisedba
- 192.168.1.2 dbb.asutus.sisedbb
- 192.168.1.3 dbc.asutus.sisedbc

Kettapaigutus ja fstab

Serverite df –h ja cat /etc/fstab väljavõte normaalolukorras

Deponeeritud kasutajanimede ja pääsuvõtmete asukoha viide

Inim- ja masinkasutajate õigused ja kus hoitakse füüsilist koopiat.

Pääsuvõtmete asukoht	ITO šeifis
Inim- ja masinkasutajate õigused	Tavakasutajad: • Nimi Administraator: • Nimi
Operatsioonisüsteemi kasutajad ja grupid	• kasutaja • root • Grupid

Tootja juhendmaterjalide asukohad

Komponentidega kaasas olevad installatsioonijuhendite ja muud tootja juhendmaterjalide asukohad (nt kriitilised juhendid paberkandjal ruumis X riiulil Y, väheolulised veebiaadressil Z)

- **ITO seifis**
- <LINK 1>
- <LINK 2>

Tarkvarakoopiate õigete versioonide asukohad

Tarkvarakoopiate õigete versioonide asukohad (nt kriitilised CD-l ruumis X riiulis Y, väheolulised veebiaadressil Z),

Taastamiseks vajaminevate konfiguratsioonifailide, krüptovõtmete asukohad.

- Asutuse failiserveri kaustas X;
- Infoturbe seifis
- <Link>

Taaste protseduurid

Järgnevalt loetleda kõik taastamisega seotud juhised ja taastamise protseduurid kujul, et taastamine on võimalik ka süsteemi detailselt mittetundva administraatori poolt.

1. samm-sammuline taastetoimingute kirjeldus. Nt väga üldsiselt:
2. võta laost asukohast A varuseade ja paigalda seadmekappi asukohta B;
3. teosta kaabeldus ja võrgukonfiguratsioon vastavalt juhisele C;
4. paigalda standardsel viisil operatsioonisüsteem D versioon x.x ja häälesta see vastavalt juhisele E;
5. paigalda toode meediumilt F, mis asub asukohas G vastavalt juhendile H;
6. paigalda varundatud andmed, varundusplaani leiab asukohast I

Organisatoorsed protseduurid

1. organisatsioonisisesed teavituskohustused;
2. lepingujärgsed kohustuslikud toimingud ja vastutajad, nt partnerite informeerimine.