					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P41					Dokumendi pealkiri: **P41**							
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:							
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu	

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

Kooskõla standardite ja õigusaktidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	6.1.3, 8.1, 9.1	
ISO/IEC 27002:2022	5.20, 5.21, 5.22, 5.23, 5.30	
NIST SP 800-53 Rev.5	SR-2, SR-3, SR-5, SR-6, SR-11, RA-3	
ELi isikuandmete kaitse üldmäärus (GDPR)	art 28, art 32 lõige 1 punkt d	
ELi NIS2	art 21 lõige 2 punkt d, art 21 lõige 3, art 22	
ELi DORA	art 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Eesmärk

1.1 Tugevdada organisatsiooni tarneahela turbepraktikaid, kehtestades protsessi kriitiliste sõltuvuste tuvastamiseks ja haldamiseks tarnijate ning teenuseosutajate suhtes, lähtudes NIS2 artiklist 21 lõikest 3 ja liidu tasandi tarneahela riskihindamistest.

1.2 Tagada, et ühe tarnija kontsentreeritud kasutamisest või temast sõltumisest tulenevad riskid on mõistetud ja maandatud ning et kõik valdkonnaspetsiifilised tarneahela riskid, millele pädevad asutused viitavad NIS2 artikli 22 alusel, on hõlmatud meie riskijuhtimises ja talitluspidevuse planeerimises.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigile olulistele tarnijatele ja teenuseosutajatele, kellele organisatsioon tugineb kriitiliste tegevuste tagamisel, eelkõige IKT tarneahelas (riistvara, tarkvara, pilveteenused, telekommunikatsioon, hallatud teenused).

2.2 See hõlmab sisemisi funktsioone, sealhulgas hanget, tarnijahaldust, riskijuhtimist ja asjakohaseid tegevusüksusi. Samuti hõlmab see tarnijaid ulatuses, mis on vajalik riskiteabe kogumiseks. „Kriitilised tarnijad“ on tarnijad, kelle tõrge või kompromiteerimine võib oluliselt mõjutada meie võimet osutada teenuseid või täita õiguslikke kohustusi.

3. Eesmärgid

3.1 Saada nähtavus tarneahela sõltuvuste üle, eelkõige tuvastada üksikud rikkepunktid või kõrge kontsentratsiooniriskiga olukorrad meie tarnijabaasis (nt sõltuvus ühest pilveteenuse osutajast kõigi teenuste osutamisel).

3.2 Rakendada meetmeid tarnijatega seotud riskide vähendamiseks ja haldamiseks, näiteks hajutamine, talitluspidevuse ajutised lahendused või nõue parandada tarnija kontrollimeetmeid, et suurendada vastupidavust tarnija tõrgete või tarneahelast lähtuvate rünnete vastu.

3.3 Viia tegevus kooskõlla NIS2 nõuetega, lõimides kriitiliste tarneahelate koordineeritud turvariskide hindamiste tulemused artikli 22 kohaselt organisatsiooni riskialastesse otsustesse ning tagades, et meie tarneahela riskikäsitlus on dokumenteeritud ja tõendatav.

4. Rollid ja vastutused

4.1 Tarnijahaldus (VMO): vastutab tarnijasõltuvuste registri eest ja koordineerib riskihindamisi. Tagab, et kasutuselevõtu käigus ja seejärel perioodiliselt hinnatakse iga võtmetarnija kriitilisust ja sõltuvuse taset.

4.2 Riskijuhtimine (ettevõtte riskikomitee): vaatab läbi kontsentratsiooniriski ja sõltuvusanalüüsid, kinnitab riskikäsitluse strateegiad (nt alternatiivse tarnija lisamise või kriitiliste komponentide lisavarude hoidmise heakskiitmine). Hõlmab tarneahela riskid üldisesse riskiregistrisse ja annab aru tippjuhtkonnale.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Seire ja audit

9.1 Sõltuvusregistrit ja riskihindamisi auditeeritakse siseauditi käigus kord aastas. Siseaudit kontrollib, et kõik kriitilised tarnijad on registris, nende riskihinnangud on ajakohased ning maandamiskavad on olemas ja edenemas. Samuti kontrollitakse, et väliste riskihindamiste sisendeid (artikli 22 aruanded jne) on nõuetekohaselt arvesse võetud.

9.2 Hajutamise ja talitluspidevuse meetmete tõhusust testitakse perioodiliselt. Näiteks võib läbi viia planeeritud simulatsiooni, kus eeldatakse olulise tarnija tõrget, et testida meie talitluspidevuse plaane ja alternatiivseid korraldusi (sarnaselt katastroofitaaste õppusega, kuid tarnija katkestuse stsenaariumi jaoks). Nende testide tulemused dokumenteeritakse ning puudused kõrvaldatakse.

9.3 Mõõdikud: riskijuhtimisfunktsioon jälgib selliseid mõõdikuid nagu „% kriitilistest teenustest, mille jaoks on olemas vähemalt üks alternatiivne tarnija või lahendus“ või „5 suurimat tarnijasõltuvust ja nende riskitrend“. Need mõõdikud lisatakse juhtkonnale esitatavatele riskitöölaudadele. Sõltuvusriski vähenemine ajas on eesmärk; kui mõõdikud näitavad sõltuvuse suurenemist, peab see käivitama juhtkonna arutelu.

10. Läbivaatamine ja ajakohastamine

10.1 Käesoleva poliitika vaatavad tarnijahalduse ja riskijuhtimise meeskonnad läbi vähemalt kord aastas. Läbivaatamisel võetakse arvesse kõik muudatused tarnijamaastikul (nt kui uus tarnija muutub kriitiliseks või varasema tarnija kasutamine lõpetatakse) ning kõik uued allhanke või kolmanda osapoole riskiga seotud õigusaktidest tulenevad nõuded.

10.2 Kui valdkondlikud asutused annavad välja ajakohastatud suuniseid või kui intsident paljastab puudujääke (näiteks kui tarnija katkestusel oli oodatust suurem mõju, mis näitab, et meie riskihindamine alahindas sõltuvust), ajakohastatakse poliitikat, et täpsustada kriteeriume või maandamisstrateegiaid.

10.3 Poliitika muudetud versioonid peab heaks kiitma tippjuhtkond. Olulised muudatused edastatakse kõigile asjakohastele üksustele ning koolitusmaterjalid ajakohastatakse vastavalt, et need kajastaksid uusi protseduure või standardeid.

11. Seotud poliitikad ja seosed

11.1 P01 – Infoturbepoliitika. Määrab vastutuse tarnijasõltuvuse juhtimise eest.

11.2 P02 – Juhtimisrollide ja vastutuste poliitika. Selgitab tarnijariskiga seotud otsuste omandit ja vastutust.

11.3 P06 – Riskijuhtimise poliitika. Hõlmab kontsentratsiooniriski ettevõtte riskiregistrites.

11.4 P26 – Kolmandate osapoolte ja tarnijate turbepoliitika. Määrab baastaseme turbenõuded; P41 lisab sõltuvuse ja kontsentratsiooni kontrollimeetmed.

11.5 P27 – Pilveteenuste kasutamise poliitika. Kohaldab sõltuvuskriteeriume pilveteenuste kasutuselevõtule ja väljumisnõuetele.

11.6 P28 – Allhankearenduse poliitika. Käsitleb sõltuvusriske välises arendustegevuses.

11.7 P32 – Talitluspidevuse ja katastroofitaaste poliitika. Kavandab tarnija tõrke või asendamise stsenaariumid.

11.8 P37 – Õigusnormidele vastavuse poliitika. Tagab, et lepingud ja kohustused kajastavad sõltuvuse kontrollimeetmeid.

12. Viited

12.1 NIS2 direktiiv (EL 2022/2555), artikkel 21 lõige 3 (nõuab iga otsese tarnija/teenuseosutaja spetsiifiliste haavatavuste ja nende küberturbe kvaliteedi arvesse võtmist, sealhulgas koordineeritud tarneahela riskihindamiste tulemusi)

12.2 NIS2 direktiiv, artikkel 22 lõige 1 (kriitiliste tarneahelate liidu tasandi koordineeritud turvariskide hindamised – annavad üksustele teavet sektoripõhiste tarnijariskide kohta)

12.3 Komisjoni rakendusmäärus (EL) 2024/2690, lisa punkt 5 (tarneahela turbenõuded üksustele, sealhulgas tarnijate valiku, hajutamise ja lepinguliste kohustuste kriteeriumid)

12.4 ENISA tarneahela küberturbe head tavad (2022) – soovitused kriitiliste tarnijate tuvastamiseks ja seotud riskide haldamiseks

12.5 ISO/IEC 27001:2022 / ISO/IEC 27002:2022