					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P26					Dokumendi pealkiri: **Kolmandate osapoolte ja tarnijate turbepoliitika**							
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	Punkt 8	Operatiivne planeerimine ja kontroll: nõuab formaalseid kontrollimeetmeid ISMS-i mõjutavate kolmandate osapoolte teenuste üle
ISO/IEC 27002:2022	Kontrollimeetmed 5.19–5.22	Tarnijasuhete poliitikad ja protseduurid; tarnijariskide haldamine; tarnijate teenuste osutamise haldamine; tarnijate seire ja läbivaatamine
NIST SP 800-53 Rev. 5	SA-9, SA-10, CA-3, PS-7	Väliste süsteemiteenuste kasutamine; arendaja konfiguratsioonihaldus; süsteemidevahelised ühendused; kolmandate osapoolte personali turve
ELi isikuandmete kaitse üldmäärus (GDPR)	Artiklid 28, 32, 33	Volitatud töötleja kohustused, töötlemise turvalisus, isikuandmete rikkumisest teatamine
ELi NIS2	Artikkel 21(2)(e–f)	Riskipõhine tarnijahaldus ja turbealane järelevalve
ELi DORA	Artiklid 28, 30	IKT kolmanda osapoole risk, kriitiliste IKT kolmandate osapoolte teenuseosutajate järelevalve
COBIT 2019	BAI05, DSS02, MEA03	Organisatsiooniliste muudatuste võimaldamise juhtimine; teenusetaotluste ja intsidentide haldamine; vastavuse seire, hindamine ja auditeerimine

1. Eesmärk

1.1 Käesolev poliitika määratleb infoturbenõuded turvaliste suhete loomiseks, haldamiseks ja ülläpidamiseks kolmandatest osapooltest tarnijate ning teenuseosutajatega.

1.2 See tagab, et kõigi tarnijate suhtes, kellel on juurdepääs organisatsiooni andmetele, süsteemidele või taristule, rakendatakse kogu teenuse elutsükli jooksul rangeid turbekontrolle, lepingulisi kaitsemeetmeid ja pidevat järelevalvet.

1.3 Poliitika toetab ISO/IEC 27001 lisa A kontrollimeetmeid 5.19 kuni 5.22, lõimides turbenõuded hankesse, kaasamisse, taustakontrolli, lepingute haldamisse, teenuste seiresse ja teenuse lõpetamise protsessidesse.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub järgmisele:

2.1.1 kõigile kolmandatest osapooltest tarnijatele, töövõtjatele, pilveteenuse osutajatele ja teenuseorganisatsioonidele, kes töötlevad organisatsiooni teabevarasid või kellel on neile juurdepääs;

2.1.2 kõigile sisemistele rollidele, kes osalevad tarnijate hindamises, tarnijate kaasamisprotsessis, lepingute sõlmimises, riskijuhtimises, seires või teenuse lõpetamises;

2.1.3 kõigile tarnijasuhetele, mis hõlmavad juurdepääsu tundlikele andmetele, integratsiooni tootmisteenustega või ärikriitiliste funktsioonide toetamist.

2.2 Poliitika hõlmab nii otseseid tarnijaid kui ka nende alltöövõtjaid, kui see on asjakohane, ning hõlmab kolmanda osapoole tarkvara, taristut, tuge ja allhanketeenuseid.

3. Eesmärgid

3.1 Tagada, et tarnijatega seotud turberiske tuvastatakse, hinnatakse ja maandatakse järjepidevalt kogu suhte elutsükli vältel.

3.2 Kehtestada kõigis tarnijalepingutes standardiseeritud turbenõuded, sealhulgas andmekaitserikkumisest teatamise kohustused, auditeerimisõigused ja andmekaitsealased vastutused.

3.3 Nõuda ametlikku taustakontrolli ja dokumenteeritud riskihindamisi enne uute tarnijate kaasamist või kõrge riskiga teenuslepingute uuendamist.

3.4 Luua mehhanismid tarnijate vastavuse pidevaks seireks, sealhulgas tulemuslikkuse hindamiseks, audititeks ja intsidentide eskaleerimiseks.

3.5 Hallata muudatusi tarnijate teenustes ning tagada teenuse lõpetamisel turvaline väljumisprotsess ja andmete tagastamine või hävitamine.

3.6 Viia kolmandate osapoolte turbekontrollid kooskõlla kohaldatavate regulatiivsete ja lepinguliste kohustustega, sealhulgas GDPR-i, NIS2, DORA ja ISO/IEC 27001 nõuetega.

4. Rollid ja vastutused

4.1 Infoturbejuht

4.1.1 Vastutab käesoleva poliitika eest ja tagab selle kooskõla üldise ISMS-i, riskijuhtimise ja vastavusstrateegiaga.

4.1.2 Kinnitab tarnijate klassifitseerimistasemed, turbeülevaatuste tulemused ja kõrge riskiga erandid.

4.1.3 Osaleb tõsiste tarnijaintsidentide eskaleerimisel ja kriitiliste teenuste lepinguläbirääkimistel.

4.2 Tarnijahaldus

4.2.1 Tagab, et kõik uued ja uuendatud tarnijalepingud sisaldavad heakskiidetud turbe- ja andmekaitseklausleid.

4.2.2 Haldab tsentraliseeritud tarnijaregistrit ja koordineerib koostööd õigus- ja vastavusfunktsiooniga seoses kolmanda osapoole riskide dokumentatsiooniga.

4.2.3 Algatab tarnija kaasamisprotsessi ja tagab kooskõla lepingueelsete turbehindamistega.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika tuleb läbi vaadata vähemalt kord aastas või varem järgmiste asjaolude korral:

9.1.1 olulised muudatused hankestrateegias või tarnijate ökosüsteemis;

9.1.2 õigus- või regulatiivse raamistiku uuendused (nt DORA, GDPR);

9.1.3 suure mõjuga kolmanda osapoole intsidendid, andmekaitserikkumised või auditi ebaõnnestumised;

9.1.4 riskihindamiste või väliste sertifitseerimisasutuste leiud.

9.2 Läbivaatamisprotsessi eest vastutavad ühiselt infoturbejuht, tarnijahaldus, õigus ja vastavus ning riskijuhtimise funktsioon.

9.3 Kõik poliitikamuudatused tuleb dokumenteerida ISMS-i dokumendihalduse registris, hallata versioonihalduse alusel ning edastada asjakohastele sidusrühmadele tarnijahalduse kanalite ja turbeteadlikkuse programmide kaudu.

9.4 Asendatud versioone tuleb jälgitavuse ja õigusaktidele vastavuse tagamiseks arhiveerida vähemalt kolm aastat.

10. Seotud poliitikad ja seosed

10.1 P1 – Infoturbepoliitika. Määratleb üldise kohustuse tagada kõigi organisatsiooni tegevuste turvalisus, sealhulgas sõltuvused kolmandatest osapooltest tarnijatest ja välistest teenuseosutajatest.

10.2 P6 – Riskijuhtimise poliitika. Suunab kolmandate osapoolte suhetega seotud riskide, sealhulgas tarnijate ökosüsteemist tulenevate päranduvate või süsteemsete riskide tuvastamist, hindamist ja maandamist.

10.3 P17 – Andmekaitse ja privaatsuspoliitika. Kohaldub kõigile tarnijatele, kes käitlevad isikuandmeid, nõudes asjakohaseid lepingutingimusi, edastamise kaitsemeetmeid ja lõimitud privaatsuse põhimõtteid.

10.4 P4 – Juurdepääsukontrolli poliitika. Määratleb, kuidas kolmandate osapoolte personal saab juurdepääsu organisatsiooni süsteemidele, rakendades rollipõhiseid õigusi, seansikontrolle ja juurdepääsu tühistamise protseduure.

10.5 P22 – Logimis- ja seirepoliitika. Nõuab, et tarnijate juurdepääsu süsteemidele seirataks, logitaks ja vaadataks läbi, eelkõige keskkondades, kus toimub privilegeeritud või andmekeskne tegevus.

10.6 P30 – Intsidentidele reageerimise poliitika (P30). Määratleb eskaleerimisprotseduurid ja rikkumisest teatamise nõuded tarnijast lähtuvate turbesündmuste või kolmanda osapoole süsteeme hõlmavate ühiste uurimiste korral.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001: Punkt 8.1 – Operatiivne planeerimine ja kontroll: nõuab formaalseid kontrollimeetmeid ISMS-i mõjutavate kolmandate osapoolte teenuste üle.

11.2 ISO/IEC 27002:2022 – Kontrollimeetmed 5.19 kuni 5.22:

11.2.1 Lisa A kontrollimeede 5.19 – Tarnijasuhete poliitikad ja protseduurid: nõuab kontrollimeetmeid tarnijasuhete haldamiseks.

11.2.2 Lisa A kontrollimeede 5.20 – Tarnijariskide haldamine: keskendub tarnijate turvaseisundi tuvastamisele, hindamisele ja jooksvale järelevalvele.

11.2.3 Lisa A kontrollimeede 5.21 – Tarnijate teenuste osutamise haldamine: nõuab tulemuslikkuse ja turbe vastavust lepingulistele ootustele.

11.2.4 Lisa A kontrollimeede 5.22 – Tarnijate seire ja läbivaatamine: rõhutab vajadust kolmandate osapoolte vastavust jooksvalt valideerida ja uuesti hinnata.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 SA-9 – Väliste süsteemiteenuste kasutamine: määratleb väliste üksuste hallatavate süsteemide turbe- ja riskinõuded.

11.3.2 SA-10 – Arendaja konfiguratsioonihaldus: kohaldub juhtudel, kui kolmandad osapooled tarnivad tarkvara või keskkondi.

11.3.3 CA-3 – Süsteemidevahelised ühendused: nõuab järelevalvet ja kokkulepet üksustevaheliste süsteemsete andmevoogude üle.

11.3.4 PS-7 – Kolmandate osapoolte personali turve: tagab, et töövõtjaid ja tarnijate personali kontrollitakse ja seiratakse asjakohaselt.

11.4 ELi isikuandmete kaitse üldmäärus (GDPR) (2016/679):

11.4.1 Artikkel 28 – Volitatud töötleja kohustused: nõuab kirjalikke kokkuleppeid andmetöötlejatega, sealhulgas tehnilisi ja korralduslikke meetmeid.

11.4.2 Artikkel 32 – Töötlemise turvalisus: nõuab asjakohaseid kaitsemeetmeid nii vastutavatelt kui ka volitatud töötlejatelt.

11.4.3 Artikkel 33 – Isikuandmete rikkumisest teatamine: nõuab tarnijatelt rikkumise korral viivitamatut teavitamist.

11.5 ELi NIS2 direktiiv (2022/2555):

11.5.1 Artikkel 21(2)(e–f): nõuab riskipõhist tarnijahaldust ja turbealast järelevalvet, eelkõige elutähtsate ja oluliste üksuste digitaalsetes tarneahelates.

11.6 ELi DORA (2022/2554):

11.6.1 Artikkel 28 – IKT kolmanda osapoole risk: kehtestab kohustused riskihindamiseks, lepingulisteks turbenõueteks ja väljumisstrateegiateks finantsteenuse osutajatele.

11.6.2 Artikkel 30 – Kriitiliste IKT kolmandate osapoolte teenuseosutajate järelevalve: kehtestab peamiste tarnijate jaoks tõhustatud seire- ja järelevalveootused.

11.7 COBIT 2019:

11.7.1 BAI05 – Organisatsiooniliste muudatuste võimaldamise juhtimine: tagab, et tarnijate üleminekuid juhitakse turvaliselt.

11.7.2 DSS02 – Teenusetaotluste ja intsidentide haldamine: kohaldub tarnijate teatatud probleemidele ja intsidentide käsitluse lõimimisele.

11.7.3 MEA03 – Vastavuse seire, hindamine ja auditeerimine: tugevdab tarnijate tulemuslikkuse mõõtmist ja vastavuse seiret.