					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P06					Dokumendi pealkiri: **Riskijuhtimise poliitika**							
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 kohaldatavate standardite ja regulatsioonidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 6.1, 8.32, 10	Riskide tuvastamise ja juhtimise alused, lõimimine muudatuste juhtimisse, pidev parendamine
ISO/IEC 27005:2024	Kogu riski elutsükli metoodika	Terviklik riskijuhtimise protsess kooskõlas standardiga
ISO 31000:2018	Riskijuhtimise põhimõtted ja raamistik	Raamistikus rakendatud riskijuhtimise põhimõtted
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Suunised ja ülesehitus riskihindamisteks, tasandipõhine riskijuhtimine
ELi isikuandmete kaitse üldmäärus (GDPR)	Artiklid 24, 25, 32	Andmekaitse riskiprotsessid ja kontrollimeetmed
ELi NIS2	Artikkel 21(2)(a–d)	Riski- ja turvahindamise kohustused
ELi DORA	Artiklid 5, 6	IKT-riskijuhtimine ja talitluspidevus
COBIT 2019	APO12, MEA	Riskijuhtimise struktuur ja järelevalve

1. Eesmärk

1.1 Käesolev poliitika kehtestab ühtse ja formaliseeritud raamistiku infoturberiskide tuvastamiseks, analüüsimiseks, hindamiseks, käsitlemiseks, seireks ja läbivaatamiseks kogu organisatsioonis.

1.2 Sellega tagatakse riskipõhiste põhimõtete järjepidev rakendamine, et kaitsta teabevarade konfidentsiaalsust, terviklust ja käideldavust kooskõlas ISO/IEC 27001:2022 punktiga 6.1 ja standardiga ISO 31000:2018.

1.3 Poliitika lõimib infoturberiskide juhtimise organisatsiooni otsustusprotsessidesse, et täita sisemisi strateegilisi eesmärke ja väliseid regulatiivseid nõudeid.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile organisatsiooni üksustele, äriprotsessidele, süsteemidele, töötajatele ja kolmandate osapoolte kaasamistele, mis on seotud teabevarade käitlemise, arendamise, säilitamise või haldamisega.

2.2 Kohaldamisala hõlmab füüsilisi, digitaalseid ja pilvekeskkonnas majutatud varasid, sealhulgas struktureeritud ja struktureerimata andmeid, rakendusi, taristut, võrke ja teenuseid.

2.3 See hõlmab infoturberiske strateegilisel, operatiivsel, projekti- ja tehnilisel tasandil ning on kohustuslik kõigile töötajatele, töövõtjatele ja teenuseosutajatele, kes osalevad ISMS-i tegevustes.

2.4 Riskijuhtimist tuleb rakendada järgmistes olukordades:

2.4.1 uue projekti või süsteemi kasutuselevõtul

2.4.1.1 oluliste muudatuste korral (nt arhitektuur, omandisuhe, protsessid)

2.4.1.2 tarnija kaasamisel ja kolmandate osapoolte lepingute sõlmimisel

2.4.1.3 intsidendile reageerimisel ja intsidendijärgsetel ülevaatustel

2.4.1.4 organisatsiooni perioodiliste riskide ülevaatuste või auditite käigus

3. Eesmärgid

3.1 Kehtestada ja rakendada korratav, kogu organisatsiooni hõlmav riskijuhtimise protsess, mis põhineb standardite ISO/IEC 27005 ja ISO 31000 metoodikatel.

3.2 Tagada, et riske tuvastatakse, analüüsitakse, hinnatakse ja käsitletakse struktureeritud ning jälgitavate meetoditega, sealhulgas riskivastutuse ja kontrollimeetmetega seoste määratlemise kaudu.

3.3 Hallata tsentraalselt riskiregistrit ja riskikäsitlusplaani versioonihalduse alusel nii, et need kajastaksid kehtivat riskistaatust, kontrollimeetmete katvust ja maandamistegevuste edenemist.

3.4 Viia riskiotsused kooskõlla dokumenteeritud riskiisu ja riskitaluvuse tasemetega ning võimaldada teadlikke juhtimisotsuseid riski aktsepteerimise, maandamise, ülekandmise või vältimise kohta.

3.5 Jälgida pidevalt riskisuundumusi, tagada riskikäsitluse tõhusus ning võimaldada ennetavaid kohandusi ohuolukorra või ärimuudatuste alusel.

4. Rollid ja vastutused

4.1 Tippjuhtkond / juhatus

4.1.1 Kiidab heaks riskijuhtimise raamistiku ning määratleb aktsepteeritava riskiisu ja riskitaluvuse piirmäärad.

4.1.2 Annab heakskiidu riskikäsitlusstrateegiatele jääkriskide puhul, mis ületavad taluvuspiiri.

4.1.3 Tagab ressursid ja järelevalve riskijuhtimise programmi tulemuslikuks toimimiseks.

4.2 ISMS-i juht / riskijuht

4.2.1 Vastutab käesoleva poliitika eest ja tagab selle kooskõla standarditega ISO/IEC 27001 ja ISO/IEC 27005.

4.2.2 Juhib organisatsiooniülest riskihindamise protsessi ning haldab riskiregistrit ja riskikäsitlusplaani.

4.2.3 Tagab võtmeriskide perioodilise läbivaatamise ja eskaleerimise tippjuhtkonnale või infoturbe juhtimissüsteemi juhtkomiteele.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika ja sellega seotud raamistik tuleb läbi vaadata kord aastas või järgmistel juhtudel:

9.1.1 pärast olulist riskisündmust või turvaintsidenti;

9.1.2 pärast märkimisväärset organisatsioonilist või tehnilist muudatust;

9.1.3 vastusena auditi leidudele või uutele regulatiivsetele nõuetele.

9.2 ISMS-i juht, riskijuht ja vastavusmeeskond vastutavad ühiselt järgmise eest:

9.2.1 läbivaatamistsükli algatamise;

9.2.2 sisendi kogumise äriüksustelt;

9.2.3 protseduuride ja piirmäärade ajakohastamise vastavalt vajadusele.

9.3 Kõik muudatused peavad olema:

9.3.1 versioonihalduses ja logitud;

9.3.2 tippjuhtkonna poolt heaks kiidetud;

9.3.3 sidusrühmadele teatavaks tehtud;

9.3.4 säilitatud auditirepositooriumis vähemalt 5 aastat.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika on vastastikuses seoses järgmiste infoturbe poliitikatega:

10.1.1 P1 – Infoturbepoliitika: määrab üldise turbejuhtimise mudeli, mille alusel käesolev riskijuhtimise poliitika toimib.

10.1.2 P2 – Juhtimisrollide ja vastutuste poliitika: määratleb vastutavad omanikud ja juhtimistasandid, millele viidatakse riskide eskaleerimise maatriksis.

10.1.3 P5 – Muudatuste juhtimise poliitika: käivitab riskide kordushindamise taristu ja organisatsiooniliste muudatuste korral.

10.1.4 P13 – Andmete klassifitseerimise ja märgistamise poliitika: toetab mõju hindamist riskide tuvastamise käigus.

10.1.5 P33 – Auditi ja vastavuse seire poliitika: valideerib poliitika järgimise, sealhulgas riskiregistri täielikkuse ja käsitluste tõendusmaterjali olemasolu.

11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on sõnaselgelt kooskõlas järgmiste standardite ja raamistikega, et tagada vastavus infoturberiskide juhtimise rahvusvahelistele headele tavadele ja regulatiivsetele ootustele.

11.2 ISO/IEC 27001:

11.2.1 Punkt 6.1: määratleb nõuded riskide ja võimaluste tuvastamiseks, sealhulgas infoturberiskide hindamise ja riskikäsitluse kogu elutsükli jaoks. Käesolev poliitika rakendab punktide 6.1 ja 6.1.2 nõudeid struktureeritud raamistiku kaudu, mis nõuab dokumenteeritud riskide tuvastamist, analüüsi, hindamist, käsitlemist ja jääkriski aktsepteerimise korda.

11.2.2 Punkt 8.32: riskipõhise mõtteviisi lõimimine muudatuste juhtimise protsessidesse tagab, et kõik olulised organisatsioonilised muudatused käivitavad formaalse riskide kordushindamise.

11.2.3 Punkt 10: pidev parendamine on lõimitud regulaarsete poliitika läbivaatamiste, riskisuundumuste analüüsi ja riskiinfost lähtuvate SoA ajakohastamiste kaudu.

11.3 ISO/IEC 27005:

11.3.1 Annab spetsialiseeritud ja üksikasjalikud suunised infoturberiskide juhtimiseks. Käesolev poliitika rakendab ISO/IEC 27005 täielikku riskiprotsessi mudelit: konteksti määratlemine, riskide tuvastamine, riskianalüüs, riski hindamine, riskikäsitlus, riski aktsepteerimine, riskikommunikatsioon, riskiseire ja läbivaatamine.

11.4 ISO 31000:

11.4.1 Käesolev poliitika lõimib ISO 31000 põhimõtted, nagu juhtkonna pühendumus, sidumine otsustamisega ja pidev parendamine. Sellega tagatakse, et riskijuhtimine on lõimitud organisatsiooni kultuuri ja tegevustesse.

11.5 NIST SP 800-30 Rev.1:

11.5.1 On kooskõlas NIST-i riskihindamiste läbiviimise juhendiga, sealhulgas ohtude tuvastamise, haavatavuste analüüsi, tõenäosuse hindamise ja mõju määramise osas. Käesoleva poliitika ülesehitus järgib NIST-i määratletud riskihindamise samme ning kohandab need nii tehnilistele kui ka äriprotsessidele.

11.6 NIST SP 800-39:

11.6.1 Toetab organisatsiooniülest riskijuhtimist, rõhutades tasandipõhist riskijuhtimist organisatsiooni, missiooni-/äriprotsessi ja infosüsteemi tasandil. Poliitika tagab, et riskivastutus on kõigil tasanditel selgelt määratletud ning hõlmab organisatsioonitasandi käsitlusstrateegiaid.

11.7 ELi isikuandmete kaitse üldmäärus (GDPR):

11.7.1 Artikkel 24: nõuab asjakohaste tehniliste ja korralduslike meetmete rakendamist, et andmekaitseriske juhitaks nõuetekohaselt; seda käsitleb käesoleva poliitika struktureeritud riskiprotsess.

11.7.2 Artikkel 25: „lõimitud ja vaikimisi andmekaitse“ on kooskõlas riskikäsitluse lõimimisega süsteemide ja protsesside kavandamisse.

11.7.3 Artikkel 32: nõuab riskipõhist lähenemist turvameetmetele; see täidetakse mõjupõhiste riskihindamiste ja kontrollimeetmete valiku kaudu.

11.8 ELi NIS2 direktiiv:

11.8.1 Artikkel 21(2)(a–d): nõuab, et üksused viiksid läbi riskihindamisi, rakendaksid riskianalüüsi poliitikaid ja tagaksid proportsionaalsed turvameetmed. Käesolev poliitika täidab neid kohustusi pideva riski elutsükli rakendamise ja dokumenteeritud juhtimise kaudu.

11.9 ELi DORA:

11.9.1 Artikkel 5: nõuab dokumenteeritud IKT-riskijuhtimise raamistikku; see on täielikult kaetud käesoleva poliitika ülesehitusega, sealhulgas SoA seostamise ja võtmeriskinäitajatega.

11.9.2 Artikkel 6: nõuab riskijuhtimise lõimimist talitluspidevuse strateegiatesse; seda käsitletakse eskaleerimismaatriksite ja kriitiliste varade jälgimise kaudu.

11.10 COBIT 2019:

11.10.1 APO12 – Riski juhtimine: vastab otseselt organisatsiooni struktureeritud riskijuhtimise lähenemise kehtestamisele, rollide määramisele, käsitluste jälgimisele ja juhatuse tasandi aruandekohustuse tagamisele.

11.10.2 MEA01 – Toimivuse ja vastavuse seire, hindamine ja auditeerimine: kajastub käesoleva poliitika fookuses trendianalüüsile, võtmeriskinäitajate seirele ja audititagasiside lõimimisele pideva parendamise tsüklitesse.