					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P02					Dokumendi pealkiri: **Juhtimisrollide ja vastutuste 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 standardite ja regulatsioonidega

Standard/regulatsioon	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 5.3; lisa A kontroll 5	
ISO/IEC 27002:2022	Kontroll 5	
NIST SP 800-53 Rev.5	PL-1 kuni PL-4, PM-1 kuni PM-13	
EL GDPR	Artiklid 5(1)(f), 24, 37	
EL NIS2	Artikkel 21(2)(a)	
EL DORA	Artikkel 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Eesmärk

1.1 Käesolev poliitika määratleb juhtimismudeli ning organisatsiooni rollid ja vastutused, mis on vajalikud tulemusliku infoturbe juhtimissüsteemi (ISMS) toimimiseks.

1.2 See kehtestab selged vastutusahelad, otsustusõigused ja eskaleerimisteed, et tagada infoturbe lõimimine organisatsiooni kõikidele tasanditele ning selle kooskõla strateegiliste ärieesmärkidega.

1.3 Käesolev poliitika rakendab standardi ISO/IEC 27001:2022 punkti 5.3 ja kontrolli A.5.2 nõudeid, tagades, et infoturbega seotud tegevuste vastutused on selgelt määratud, dokumenteeritud, teatavaks tehtud ja perioodiliselt üle vaadatud.

1.4 Käesolev poliitika loob aluse ka lõimitud juhtimisele teiste valdkondadega, nagu riskijuhtimine, vastavus, IT käitlus ja õigus.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigile isikutele ja üksustele, kes osalevad infoturbe juhtimises, toimimises ja järelevalves ISMS-i kohaldamisala piires. See hõlmab järgmisi osapooli:

2.1.1 tegevjuhtkond, tippjuhtkond ja nõukogu liikmed

2.1.2 ISMS-i juhid, CISO-d ja kontrollide omanikud

2.1.3 protsessi- ja varaomanikud

2.1.4 alltöövõtjad ja kolmandatest osapooltest teenuseosutajad, kellele on delegeeritud infoturbega seotud vastutused

2.2 See hõlmab nii organisatsioonisiseseid kui ka sisseostetud funktsioone (nt sisseostetud SOC, pilveplatvormi administraatorid), kui juhtimisrollid on ametlikult määratud või lepinguliselt sätestatud.

2.3 Käesolev poliitika kehtib ka organisatsiooni üksustele, osakondadele ja projektimeeskondadele, kes haldavad või mõjutavad infoturbe seisukohast olulisi varasid, süsteeme või teenuseid.

3. Eesmärgid

3.1 Tagada, et infoturbe rollid ja vastutused on ametlikult määratletud, määratud, teatavaks tehtud ja dokumenteeritud.

3.2 Hoida juhtimismudelit, mis tagab tööülesannete lahususe, välistab huvide konfliktid ja võimaldab lahendamata infoturbeküsimuste eskaleerimist.

3.3 Tagada, et vastutus ja otsustusõigus infoturbealaste otsuste tegemisel on jaotatud kooskõlas ärimõju ja organisatsiooni struktuuriga.

3.4 Luua raamistik delegeerimiste, rollimuudatuste ja määratud vastutuste läbivaatamise haldamiseks.

3.5 Anda sidusrühmadele, sealhulgas regulaatoritele, audiitoritele ja klientidele, kindlus, et infoturvet juhitakse tulemuslikult ja kooskõlas kohaldatavate standarditega.

4. Rollid ja vastutused

4.1 Täitevjuhtkond (tippjuhtkond)

4.1.1 Tagab strateegilise järelevalve, eraldab ressursid ja kindlustab ISMS-i eesmärkide kooskõla ärieesmärkidega.

4.1.2 Kinnitab peamised ISMS-i dokumendid, sealhulgas infoturbepoliitika, riskitöötlusplaanid ja auditite parandusmeetmete otsused.

4.1.3 Osaleb ISMS-i juhtkonnapoolsetes ülevaatustes ja eskaleerib otsused, mis vajavad nõukogu tasandi heakskiitu.

4.1.4 Edendab turvakultuuri ja toetab infoturbe juhtimise põhimõtete järgimist kogu organisatsioonis.

4.2 Infoturbe juhtkomitee (ISSC)

4.2.1 Tegutseb ISMS-i järelevalve valdkondadeülese juhtorganina.

4.2.2 Vaatab läbi riskipositsiooni, kontrollide toimivuse, auditileiud ja strateegilised infoturbealgatused.

4.2.3 Toetab osakondadevahelist koordineerimist (nt IT, õigus, personal, riskijuhtimine, vastavus, käitlus).

4.2.4 Kinnitab eskaleerimise piirmäärad, eelarvelised eraldised ja poliitikamuudatused, mis vajavad täitevjuhtkonna sisendit.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Läbivaatamise ajakava

9.1.1 Käesolev poliitika tuleb läbi vaadata vähemalt kord aastas või järgmiste asjaolude ilmnemisel:

9.1.1.1 muudatused organisatsiooni struktuuris või täitevjuhtkonnas

9.1.1.2 ISMS-i kohaldamisala laiendamine või ümbermääratlemine

9.1.1.3 regulatiivsed muudatused, mis mõjutavad rollide määramist või järelevalvet

9.1.1.4 olulised auditileiud või intsidendid, mis on seotud juhtimise tõrkega

9.2 Läbivaatamise ja kinnitamise protsess

9.2.1 ISMS-i juht algatab ja juhib läbivaatamise protsessi, sealhulgas sidusrühmade sisendi ja audititagasiside kogumist.

9.2.2 Kavandatud muudatused vaatab läbi ISSC ning need kinnitab ametlikult täitevjuhtkond.

9.2.3 Iga versioon tuleb kajastada ISMS-i dokumendiregistris ja see peab sisaldama järgmist metaandmestikku:

9.2.3.1 poliitika tunnus ja pealkiri

9.2.3.2 versiooninumber ja muudatuste kokkuvõte

9.2.3.3 jõustumiskuupäev ja järgmise läbivaatamise kuupäev

9.2.3.4 poliitika omanik ja kinnitaja

9.2.3.5 dokumendi klassifitseerimistase

9.2.3.6 säilitamise ja arhiveerimise ajalugu

10. Seotud poliitikad ja seosed

10.1 Käesolevat poliitikat tuleb tõlgendada koos järgmiste poliitikatega:

10.1.1 P1 – Infoturbepoliitika: kehtestab üldise infoturbeprogrammi ja kirjeldab juhtkonna vastutusi poliitika kinnitamisel ning strateegilise järelevalve tagamisel.

10.1.2 P5 – Muudatuste halduse poliitika: tagab, et juhtimisstruktuuride, rollide või vastutuste muudatused läbivad dokumenteeritud heakskiidu ja riskide läbivaatamise.

10.1.3 P6 – Riskijuhtimise poliitika: tuvastab ja käsitleb juhtimisriske, mis tulenevad rollikonfliktidest, määramata ülesannetest või eskaleerimise puudumisest.

10.1.4 P7 – Tööle asumise ja töösuhte lõpetamise poliitika: rakendab kontrollide määramise ja tühistamise protsesse personali elutsükli muutuste ajal.

10.1.5 P33 – Auditi ja vastavuse seire poliitika: toetab juhtimise tulemuslikkuse sõltumatut ülevaatust ja tagab parandusmeetmete rakendamise mittevastavuse korral.

10.2 Need poliitikad toetavad ühiselt ühtset ja rakendatavat ISMS-i juhtimisraamistikku.

11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on kooskõlas rahvusvaheliselt tunnustatud infoturbe juhtimise ja rollipõhise vastutuse standardite ning raamistikega. See tagab jälgitavuse regulatiivsete ja sertifitseerimisnõueteni ning toetab põhjendatavat ISMS-i struktuuri.

11.2 ISO/IEC 27001

11.2.1 Punkt 5.3 – Organisatsiooni rollid, vastutused ja volitused: käesolev poliitika täidab nõude, et infoturbega seotud rollid oleksid selgelt määratud, teatavaks tehtud ja dokumenteeritud.

11.2.2 Punkt 9.3 – Juhtkonnapoolne ülevaatus: käesolev poliitika tagab täitevjuhtkonna järelevalve ISMS-i rollide ja juhtimise üle kvartaalse ning iga-aastase ülevaatuse kaudu.

11.2.3 Lisa A kontroll 5.2 – Infoturbe rollid ja vastutused: määratleb rollid tehnilisel, operatiivsel ja strateegilisel tasandil, et tagada tööülesannete lahusus, riskide omaniklus ja jälgitav vastutus.

11.3 ISO/IEC 27002:2022 – kontroll 5

11.3.1 Annab rakendussuunised infoturbega seotud vastutuste määramiseks kogu organisatsioonis. Käesolev poliitika võtab need suunised üle, määratledes rollitüübid, delegeerimisreeglid, eskaleerimisprotseduurid ja ülevaatusmehhanismid.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 kuni PL-4: rõhutavad ametliku planeerimisdokumentatsiooni vajadust, sealhulgas poliitikaid, mis määratlevad juhtimise ja määravad infoturbega seotud vastutused.

11.4.2 PM-1 (infoturbeprogrammi plaan) ja PM-2 (vanem infoturbejuht): kajastuvad käesolevas poliitikas CISO/ISMS-i juhi ning ametlike juhtimisrollide määramise kaudu.

11.4.3 PM-5 kuni PM-13: käesolev poliitika täidab rollide dokumenteerimise, ettevõtteüleste riskirollide, konfiguratsioonihalduse järelevalve ja põhitegevuste/ärifunktsioonidega lõimimise nõudeid.

11.5 EL GDPR (2016/679)

11.5.1 Artikkel 5(1)(f): nõuab isikuandmete kaitset loata või õigusvastase töötlemise eest. Käesolev poliitika tagab, et andmekaitse eest vastutavad isikud on selgelt määratud ja nende tegevus on järelevalve all.

11.5.2 Artikkel 24: nõuab asjakohaseid organisatsioonilisi meetmeid, sealhulgas juhtimisstruktuure.

11.5.3 Artikkel 37: nõuab andmekaitseametniku (DPO) määramist, mis peab kajastuma organisatsiooni juhtimisraamistikus ja vastutuste registris.

11.6 EL NIS2 direktiiv (2022/2555)

11.6.1 Artikkel 21(2)(a): kohustab üksusi rakendama riskianalüüsi ja infosüsteemide turvalisuse poliitikaid, sealhulgas rollipõhiseid vastutusi. Käesolev poliitika määratleb need rollid ja nende juhtimismehhanismid.

11.7 EL DORA (2022/2554)

11.7.1 Artikkel 5 – juhtimise ja sisekontrolli raamistik: nõuab IKT-riskijuhtimise vastutuste, otsustusrollide ja aruandluskanalite ametlikku määramist. Käesolev poliitika loob aluse infoturbega seotud rollide juhtimiseks IKT-keskkondades.

11.8 COBIT 2019

11.8.1 EDM01 – Tagatud juhtimisraamistiku kehtestamine: käesolev poliitika tagab, et ISMS-il on selgelt määratletud juhtimisstruktuur, mis on kooskõlas organisatsiooni vajadustega.

11.8.2 EDM02 – Tagatud kasu saavutamine: viib rollipõhised infoturbetegevused kooskõlla strateegiliste ja operatiivsete eesmärkidega, tagades vastutuse ja mõõdetavad tulemused.

11.8.3 APO01 – Hallatud I&T juhtimisraamistik ja APO12 – Hallatud risk: käesolev poliitika toetab infoturbe rollide struktureeritud juhtimist laiemas IT juhtimise ja riskiraamistikus.

11.8.4 MEA01 – Tulemuslikkuse seire, hindamine ja analüüs: lõimib ülevaatusmehhanismid, et kontrollida, kas juhtimisrollid on tulemuslikud, ajakohased ja rakendatud.