					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P01					Dokumendi pealkiri: **Infoturbepoliitika**							
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**

1. Eesmärk

1.1 Käesolev poliitika sätestab organisatsiooni üldise pühendumuse infoturbele, kehtestades ametliku infoturbe juhtimissüsteemi (ISMS).

1.2 See annab strateegilise suuna ja baasnõuded kõigi teabevarade konfidentsiaalsuse, tervikluse, käideldavuse ja toimepidevuse kaitseks füüsilistes, digitaalsetes ja pilvekeskkondades.

1.3 Käesolev poliitika täidab standardi ISO/IEC 27001:2022 punktide 5.1 ja 5.2 nõudeid, väljendades juhtkonna tahet, tippjuhtkonna pühendumust ning infoturbetegevuste kooskõla organisatsiooni eesmärkidega.

1.4 See on ISMSi raames kõigi alamate poliitikate, standardite ja protseduuride autoriteetne alusdokument ning on hädavajalik riskipõhise, vastavusele suunatud ja pidevalt paraneva turbekeskkonna tagamiseks.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigile ISMSi kohaldamisalas määratletud isikutele, varadele ja protsessidele, sealhulgas:

2.1.1 kõigile äriüksustele, osakondadele, tütarettevõtjatele ja filiaalidele

2.1.2 töötajatele, töövõtjatele, ajutistele töötajatele, konsultantidele ja kolmandatest isikutest teenuseosutajatele

2.1.3 kõigile andmetele, infosüsteemidele, rakendustele, taristule ja sidekanalitele

2.1.4 kõigile füüsilistele, pilvepõhistele, kaug- ja hübriidkeskkondadele, kus ettevõtte andmeid töödeldakse või neile pääsetakse ligi

2.2 Poliitika on siduv kõigile üksustele, kes käitlevad organisatsiooni teavet, ning kehtib teabe kogu elutsükli ulatuses alates loomisest ja edastamisest kuni säilitamise ja hävitamiseni.

2.3 Kõik erandid või piirangud selle kohaldamisala suhtes tuleb dokumenteerida ISMSi kohaldamisala kirjelduses ning põhjendada tippjuhtkonna ametliku heakskiiduga.

3. Eesmärgid

3.1 Kehtestada standardiga ISO/IEC 27001:2022 kooskõlas olev ISMS, mis toetab riskipõhist otsustamist kogu organisatsioonis.

3.2 Tagada, et konfidentsiaalsuse, tervikluse ja käideldavuse põhimõtted on lõimitud kõigisse organisatsiooni tegevustesse, süsteemidesse ja partnerlussuhetesse.

3.3 Tagada vastavus regulatiivsetele ja lepingulistele nõuetele, määratledes mõõdetavad, poliitikast lähtuvad infoturbe eesmärgid ja lõimides need äritegevusse.

3.4 Vähendada infoturbeintsidentide tõenäosust ja mõju tõhusate ennetavate, tuvastavate ja korrigeerivate kontrollimeetmete kaudu.

3.5 Edendada infoturbe küpsuse pidevat parendamist määratletud tulemusnäitajate, audititulemuste ja juhtkonna läbivaatuste kaudu.

3.6 Edendada vastutuse, teadlikkuse ja toimepidevuse kultuuri, kus kõik töötajad mõistavad oma turbega seotud kohustusi ja täidavad neid.

4. Rollid ja vastutus

4.1 Tippjuhtkond

4.1.1 Kiidab heaks infoturbepoliitika ja ISMSi raamistiku.

4.1.2 Tagab infoturbe eesmärkide kooskõla äristrateegiaga.

4.1.3 Näitab isiklikku eeskuju ja edendab tugevat infoturbekultuuri.

4.1.4 Vaatab läbi ja kiidab heaks olulised muudatused ISMSi kohaldamisalas, riskikäsitluses ja juhtimisstruktuuris.

4.2 Infoturbejuht (CISO) / ISMSi juht

4.2.1 Vastutab ISMSi toimimise eest ja tagab käesoleva poliitika kooskõla standardiga ISO/IEC 27001.

4.2.2 Juhib riskihindamise, kontrollimeetmete rakendamise ja pideva parendamise protsesse.

4.2.3 Tagab infoturbetegevuste valdkonnaülese koordineerimise ja teeb järelevalvet alamate poliitikate üle.

4.2.4 Annab tippjuhtkonnale aru ISMSi seisundist, intsidentidest, audititulemustest ja mõõdikutest.

4.2.5 Tagab, et poliitika läbivaatamine ja ajakohastamine toimub vastavalt käesoleva dokumendi punktile 9.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Läbivaatamise sagedus

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

9.1.1.1 olulised muudatused õiguslikes, regulatiivsetes või lepingulistes kohustustes

9.1.1.2 olulised muudatused organisatsiooni riskiprofiilis

9.1.1.3 sise- või välisauditite tulemused

9.1.1.4 olulised intsidendid või kontrollimeetmete tõrked

9.2 Läbivaatamise vastutus ja protsess

9.2.1 Läbivaatamise protsessi juhib CISO või määratud ISMSi juht.

9.2.2 Läbivaatamise sisend peab hõlmama järgmist:

9.2.2.1 siseauditi tulemused

9.2.2.2 riskihindamise trendid

9.2.2.3 äri- ja tehnoloogiaprotsesside muudatused

9.2.2.4 KPIde ja riskilävede täitmise tulemused

9.2.3 Kõik ajakohastused peavad:

9.2.3.1 olema versioonihallatud ja dokumenteeritud

9.2.3.2 olema tippjuhtkonna poolt heaks kiidetud

9.2.3.3 olema ametlike teavituskanalite kaudu edastatud kõigile mõjutatud osapooltele

9.2.3.4 käivitama vajalikud ajakohastused alamates dokumentides ja koolitustes

10. Seotud poliitikad ja seosed

10.1 Käesolev alusdokument on otseselt seotud järgmiste organisatsiooni turbepoliitikate ja raamistikega:

10.1.1 P2 – Juhtimisrollide ja vastutuse poliitika: määratleb käesolevas dokumendis viidatud juhtimisstruktuuri ja volituste hierarhia.

10.1.2 P3 – Lubatava kasutuse poliitika: kehtestab käitumisnõuded ja teabevarade lubatava käitlemise nõuded.

10.1.3 P4 – Juurdepääsukontrolli poliitika: rakendab käesolevast üldpoliitikast tulenevad juurdepääsuga seotud kontrollimeetmed.

10.1.4 P6 – Riskijuhtimise poliitika: annab riskipõhise raamistiku kontrollimeetmete valikuks ja jääkriskide aktsepteerimiseks.

10.1.5 P33 – Auditi ja vastavusseire poliitika: kirjeldab, kuidas sisemised kindlusmehhanismid valideerivad poliitika rakendamist.

10.2 Need vastastikused seosed tagavad ISMSi ulatuses tervikliku kooskõla ja jälgitavuse ning toetavad ühtset riskide ja vastavuse juhtimist.

11. Viitestandardid ja raamistikud

11.1 Käesolev infoturbepoliitika on ametlikult kooskõlas järgmiste standardite ja raamistikega, et tagada täielik vastavus, auditivalmidus ja regulatiivne kaitstavus:

11.2 ISO/IEC 27001

11.2.1 Punkt 5.1 – Eestvedamine ja pühendumus: käesolev poliitika näitab tippjuhtkonna pühendumust infoturbele ning määratleb ISMSiga seotud vastutused ja ressursside jaotuse.

11.2.2 Punkt 5.2 – Infoturbepoliitika: käesolev dokument on organisatsiooni ametlik turbepoliitika, mis on kooskõlas määratletud turbe-eesmärkide, äristrateegia ja standardi ISO/IEC 27001 nõuetega.

11.2.3 Punkt 6.1 – Riskide ja võimaluste käsitlemise tegevused: käesolevas poliitikas kajastuv riskipõhine lähenemine tagab, et turberessursse rakendatakse ohtudega proportsionaalselt.

11.2.4 Punkt 9.2 – Siseaudit ja punkt 10 – Parendamine: käesolev poliitika on lõimitud organisatsiooni pideva parendamise tsüklisse ja allub siseauditi valideerimisele.

11.2.5 ISO/IEC 27002:2022 – Kontrollimeede 5.1: annab juhised turbepoliitikate kehtestamiseks ja ajakohasena hoidmiseks. Käesolev poliitika järgib ISO 27002 soovitusi hierarhilise dokumentatsiooni, läbivaatamistsüklite ja rakendatavuse osas.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (turbeplaneerimise poliitika ja protseduurid): käesolev poliitika täidab nõude töötada välja, avalikustada ja läbi vaadata ametlik kogu organisatsiooni hõlmav infoturbepoliitika.

11.3.2 PM-1 kuni PM-5: käsitleb programmi tasandi juhtimist, sealhulgas infoturbe rolle, ressursside jaotust, riskistrateegiat ja turbeplaneerimise lõimimist organisatsiooni tegevusse.

11.4 ELi GDPR (2016/679)

11.4.1 Artikkel 5(2): kehtestab vastutuse põhimõtte. Käesolev poliitika määratleb vastutavad osapooled ja jälgitavad rakendustegevused.

11.4.2 Artikkel 24: nõuab riskiga kooskõlas olevate tehniliste ja korralduslike meetmete, sealhulgas poliitikate, rakendamist.

11.4.3 Artikkel 32: toetab asjakohaste meetmete rakendamist isikuandmete turvalisuse tagamiseks kogu nende elutsükli jooksul.

11.5 ELi NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(a): kohustab üksusi rakendama dokumenteeritud turbepoliitikat, mis käsitleb riskijuhtimist ja juhtimist. Käesolev poliitika täidab selle nõude ning toetab laiemat küberturbevalmidust ja elutähtsa taristu kaitset.

11.6 ELi DORA (2022/2554)

11.6.1 Artikkel 5(2): nõuab IKT-riskijuhtimise jaoks dokumenteeritud sisekontrolliraamistikku. Käesolev poliitika toetab finantssektori vastavust, määrates rollid, kontrollimeetmed ja järelevalvefunktsioonid kooskõlas DORA juhtimisootustega.

11.7 COBIT 2019

11.7.1 EDM01 – Juhtimisraamistiku kehtestamine: käesolev poliitika toetab organisatsiooni juhtimist, määratledes ISMSi rollid, juhtkonna pühendumuse ja strateegilised eesmärgid.

11.7.2 APO01 – Juhtimisraamistik: toetab struktureeritud ISMSi kehtestamist ja toimimist.

11.7.3 APO12 – Riskijuhtimine: loob aluse infoturbe riskide juhtimisele.

11.7.4 MEA01/MEA03 – Seire, hindamine ja ülevaatus: tugevdab toimivuse pidevat hindamist ja sisekontrolli seiret poliitika järgimise kaudu.