					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P06S					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**

Kohaldatavate standardite ja õigusnormidega kooskõlas

Standard/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 kuni RA-7, PM-9	
ELi NIS2	Artikkel 21(2)(a–d)	
ELi DORA	Artikkel 5	
COBIT 2019	APO12, MEA01	

1. Eesmärk

1.1 Käesolev poliitika määratleb, kuidas organisatsioon tuvastab, hindab ja juhib infoturbe, tegevuse, tehnoloogia ning kolmandate osapoolte teenustega seotud riske.

1.2 See tagab, et riskijuhtimise protsess on kooskõlas standarditega ISO 27001, ISO 31000 ja regulatiivsete nõuetega ning on planeerimise, projektide elluviimise, tarnijate valiku ja intsidentidele reageerimise lahutamatu osa.

1.3 Poliitika toetab teadlikku otsustamist, teabevarade kaitset ja peamiste äritegevuste toimepidevust.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub järgmisele:

2.1.1 kõigile organisatsiooni osakondadele, süsteemidele ja kasutajatele

2.1.2 kogu teabele, teenustele ja varadele, mida hallatakse organisatsioonisiseselt või kolmandate osapoolte kaudu

2.1.3 riskiga seotud tegevustele, sealhulgas projektide ülevaatustele, süsteemimuudatustele, allhankele ja õigusnormidele vastavuse tagamisele

2.2 See hõlmab kõiki riskiliike, sealhulgas:

2.2.1 küberturbeohte ja süsteemide haavatavusi

2.2.2 tegevushäireid ja teenusekatkestusi

2.2.3 õiguslikke, vastavus- või mainekahjuga seotud riske

2.2.4 kolmandate osapoolte ja tarneahela riske

2.3 Kõik töötajad, töövõtjad ja teenuseosutajad peavad käesolevat poliitikat järgima riskide tuvastamisel ja neist teavitamisel.

3. Eesmärgid

3.1 Lõimida lihtsad ja korratavad riskihindamise protseduurid igapäevastesse äritegevustesse.

3.2 Tuvastada ja seada tähtsuse järjekorda riskid, mis võivad mõjutada konfidentsiaalsust, terviklust ja käideldavust või õigusnormidele vastavust.

3.3 Määrata kõigile olulistele riskidele vastutaja ja määratleda riskikäsitlusmeetmed.

3.4 Hoida riskiregister täpse ja ajakohasena, et tagada auditivalmidus ja toetada riskide seiret.

3.5 Tagada juhtkonna osalus riskitaluvuse ja oluliste käsitlusplaanide heakskiitmisel.

4. Rollid ja vastutus

4.1 Tegevjuht

4.1.1 määrab organisatsiooni riskiisu ja kinnitab riskijuhtimise raamistiku.

4.1.2 kiidab heaks olulised riskikäsitlust puudutavad otsused ja vajalikud ressursid.

4.1.3 vaatab koos riskikoordinaatoriga kord kvartalis üle peamised riskid.

4.2 Riskikoordinaator (või ISMS-i omanik)

4.2.1 koordineerib riskihindamisi ja haldab riskiregistrit.

4.2.2 tagab, et riskide skoorimine, riskivastutus ja riskikäsitlusmeetmed on dokumenteeritud.

4.2.3 korraldab vähemalt ühe ametliku riskide ülevaatuse aastas.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Iga-aastane poliitika läbivaatamine

9.1.1 käesolev poliitika tuleb vähemalt kord aastas tegevjuhi ja riskikoordinaatori poolt läbi vaadata, et tagada selle asjakohasus ja täielikkus.

9.2 Ajakohastamise käivitajad

9.2.1 varasem läbivaatamine ja ajakohastamine tuleb teha järgmistel juhtudel:

9.2.1.1 oluline intsident või auditi leiud toovad esile puudujäägid riskijuhtimises

9.2.1.2 kasutusele võetakse uued äriüksused, tehnoloogiad või partnerlussuhted

9.2.1.3 muutub õigusnormidest või lepingust tulenev nõue

9.3 Versioonihaldus

9.3.1 kõik selle poliitika muudatused tuleb versioonihalduses registreerida järgmise metaandmestikuga:

9.3.1.1 versiooninumber ja jõustumiskuupäev

9.3.1.2 muudatuste kokkuvõte

9.3.1.3 kinnitaja (tegevjuht)

9.3.1.4 auditi eesmärgil arhiveeritud varasemad versioonid

9.4 Teabevahetus ja teadlikkus

9.4.1 poliitika ajakohastatud versioonid ja olulised riskikäsitlusplaanid tuleb edastada mõjutatud töötajatele. Iga-aastane teadlikkuse tõstmise koolitus peab hõlmama riskiteadlikkuse aluspõhimõtteid.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika toimib koordineeritult mitme teise poliitikaga, et tagada terviklik turbejuhtimine:

10.1.1 P2S – Juhtimisrollide ja vastutuste poliitika: määratleb, kes vastutab riskivastutuse ja otsustamise eest.

10.1.2 P5S – Muudatuste juhtimise poliitika: nõuab riskihindamist enne tehniliste või protsessimuudatuste rakendamist.

10.1.3 P17S – Andmekaitse ja privaatsuse poliitika: käsitleb isikuandmete töötlemisega seotud regulatiivset riski.

10.1.4 P30S – Intsidentidele reageerimise poliitika (P30): tagab, et riskikäsitlus jätkub turvaintsidentide ajal ja järel.

10.1.5 P33S – Tegevuse järjepidevuse poliitika: tuvastab jääkriskid ja taastemeetmed kriitiliste teenuste jaoks.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 6.1 – kehtestab ametliku riskijuhtimise protsessi ja riskikäsitluse kavandamise.

11.1.2 Punkt 6.1.3 – nõuab organisatsioonilt dokumenteeritud käsitlusplaanide ja heakskiitude säilitamist.

11.2 ISO/IEC 27002

11.2.1 Kontrollimeetmed 5.4 ja 5.25 – annavad rakendussuunised riskivastutuse, prioriseerimise ja elutsükli haldamise kohta.

11.3 NIST SP 800-53 Rev. 5

11.3.1 RA-1 kuni RA-7 – määratlevad riskihindamise, reageerimisstrateegiad, dokumenteerimise ja läbivaatamise mehhanismid.

11.4 PM-9

11.4.1 nõuab organisatsiooni riskide järjepidevat juhtkonnatasandi järelevalvet.

11.5 ELi NIS2 direktiiv

11.5.1 Artikkel 21(2)(a–d) – kehtestab olulistele ja tähtsatele üksustele kohustuslikud riskihindamise, riskide maandamise ja juhtimise kontrollimeetmed.

11.6 ELi DORA

11.6.1 Artikkel 5 – nõuab reguleeritud üksustelt IKT-riskijuhtimise raamistiku määratlemist ja haldamist, sealhulgas tuvastamist, klassifitseerimist ja reageerimist.

11.7 COBIT 2019

11.7.1 APO12 – Manage Risk: lõimib riski strateegilisse ja operatiivsesse planeerimisse.

11.7.2 MEA01 – Monitor, Evaluate, and Assess: tagab riskiprotsesside ja tegevuste tõhususe ning vastavuse.