					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P01S					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**

Kooskõla standardite ja õigusnormidega

Standard/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 5.1, 5.2, 5.3, 6.1, 6.2, 8	Määratleb juhtkonna pühendumuse, poliitikanõuded, rollide määramise, riskihindamise ja operatiivjuhtimise nõuded
ISO/IEC 27002:2022	Kontrollmeetmed 5.1–5.5	Määratleb dokumenteeritud infoturbepoliitikate koostamise, rollide määramise, tööülesannete lahususe ja juhtkonna vastutuse
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Sätestab nõuded turbeprogrammi kavale, turbeplaneerimise poliitikale, hindamisele ja autoriseerimisele ning juurdepääsukontrollile
ELi isikuandmete kaitse üldmäärus (2016/679)	Artikkel 5(2), artikkel 32	Vastutuse põhimõte ja töötlemise turvalisuse meetmed, eelkõige dokumenteeritud rollide osas
ELi NIS2 direktiiv (2022/2555)	Artikkel 21(2)(a)	Nõuab küberriskide juhtimiseks riskijuhtimismeetmeid, rolle ja vastutusi
ELi DORA määrus (2022/2554)	Artikkel 9, artikkel 10	Nõuab rollide määramist IKT-riskide juhtimiseks ja talitluspidevuse tagamiseks
COBIT 2019	EDM03, APO13, DSS05	Toetab riskide optimeerimist, turbe juhtimist ja turbeteenuste juhtimist selge rollijaotuse kaudu

1. Eesmärk

1.1 Käesolev poliitika väljendab organisatsiooni pühendumust kliendi- ja äriteabe kaitsele, määratledes selged vastutused ja praktilised turvameetmed, mis sobivad ka organisatsioonidele, kellel puudub eraldiseisev IT-meeskond.

1.2 See tagab, et kõik töötajad, töövõtjad ja teenusepakkujad järgivad siduvaid nõudeid, et täita ISO/IEC 27001 sertifitseerimise nõuded täies ulatuses.

1.3 Käesolev poliitika võimaldab organisatsioonil suurendada klientide usaldust, näidates selgelt, kuidas nende teavet kaitstakse määratletud vastutuste, struktureeritud protsesside ja selge vastutusahela kaudu.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigile isikutele, kes pääsevad ligi organisatsiooni andmetele ja süsteemidele või haldavad neid, sealhulgas:

2.1.1 ettevõtte omanikud ja tegevjuhid

2.1.2 töötajad, töövõtjad ja praktikandid

2.1.3 välised IT-teenusepakkujad või konsultandid

2.2 See hõlmab kõiki teabe, süsteemide ja teenuste liike, sealhulgas:

2.2.1 äridokumendid, kliendiandmed, paroolid ja e-kirjad

2.2.2 IT-seadmed, näiteks sülearvutid ja telefonid

2.2.3 failide talletamiseks, suhtluseks või finantstoiminguteks kasutatavad pilveteenused

2.2.4 kontoriruumides säilitatavad füüsilised dokumendid

2.3 Poliitika kehtib kõigis töökeskkondades – kontoris, kaugtööl ja pilvekeskkonnas – ning hõlmab kõiki seadmeid ja tarkvara, mida kasutatakse äriteabe töötlemiseks või säilitamiseks.

3. Eesmärgid

3.1 Selge vastutuse määramine: tuleb tagada, et infoturbe eest on alati määratud vastutaja. Tavaliselt on selleks tegevjuht või tema poolt ametlikult määratud isik.

3.2 Kliendi- ja äriteabe kaitse: tuleb rakendada usaldusväärseid ja järjepidevaid kaitsemeetmeid, et vältida tundlike andmete, sealhulgas kliendi- ja finantsandmete, väärkasutust, kadu või vargust.

3.3 ISO/IEC 27001 sertifitseerimise toetamine: organisatsioon peab suutma tõendada täielikku vastavust ISO/IEC 27001 nõuetele ning olema auditiks valmis ja sertifitseerimiseks sobiv ka ilma keeruka taristuta.

3.4 Turbe lõimimine äritegevusse: infoturve tuleb lõimida organisatsiooni igapäevategevustesse ja otsustusprotsessidesse.

3.5 Turvateadlikkuse ja -kultuuri kujundamine: tuleb tagada, et iga töötaja mõistab ja järgib turvapraktikaid, näiteks tugevate paroolide kasutamist ja kahtlasest tegevusest teatamist.

4. Rollid ja vastutused

4.1 Tegevjuht või ettevõtte omanik

4.1.1 Vastutab täielikult infoturbe eest.

4.1.2 Kinnitab käesoleva poliitika ja hoiab selle ajakohasena.

4.1.3 Tagab, et kõik peamised turbeülesanded täidetakse kas vahetult või kirjalikult delegeerituna.

4.1.4 Kontrollib, et kõik delegeeritud turbeülesanded (näiteks juurdepääsu haldamine või intsidentidele reageerimine) täidetakse tulemuslikult.

4.1.5 On vaikimisi kontaktisik kõigis sise- ja välistes turbeküsimustes, sealhulgas auditite ja klientide päringute korral.

4.1.6 Jälgib iga-aastase läbivaatamise käigus edenemist eesmärkide täitmisel. Eesmärgid peavad võimaluse korral olema mõõdetavad (nt koolitatud töötajate osakaal, raporteeritud intsidentide arv) ning neid tuleb ajakohastada turbeleidude ja riskimuutuste põhjal.

4.2 Määratud töötaja (kui asjakohane)

4.2.1 Võib toetada tegevjuhti igapäevaste ülesannete täitmisel, näiteks kasutajakontode loomisel, lahkujate juurdepääsu eemaldamisel või IT-teenusepakkujaga koordineerimisel.

4.2.2 Peab olema ametlikult määratud ning tal peavad olema ülesannete täitmiseks piisavad volitused ja töövahendid.

4.2.3 Teavitab kõigist probleemidest tegevjuhti.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Iga-aastane läbivaatamine

9.1.1 Tegevjuht peab käesoleva poliitika läbi vaatama vähemalt kord aastas, et tagada jätkuv vastavus ISO/IEC 27001 sertifitseerimise nõuetele, regulatiivsetele muudatustele (nt isikuandmete kaitse üldmäärus, NIS2 ja DORA) ning muutuvatele ärivajadustele.

9.2 Vahepealsed läbivaatamised

9.2.1 Täiendavad läbivaatamised tuleb teha alati, kui toimuvad olulised muudatused, näiteks:

9.2.1.1 ulatuslikud turvaintsidendid või rikkumised

9.2.1.2 uute äriprotsesside või tehnoloogiate kasutuselevõtt (nt uus tarkvara, kaugtööplatvormid või pilveteenused)

9.2.1.3 teabe käitlemist mõjutavate õiguslike või regulatiivsete nõuete muutused

9.3 Muudatuste dokumenteerimine

9.3.1 Kõik poliitika läbivaatamised ja muudatused tuleb ametlikult dokumenteerida, märkides selgelt kuupäeva, muudatuste sisu ja tegevjuhi kinnituse.

9.3.2 Poliitika versiooniajalugu tuleb säilitada turvaliselt, et auditi käigus oleks võimalik tõendada poliitika arengut ja vastavust.

9.4 Muudatuste teatavakstegemine

9.4.1 Kõik käesoleva poliitika muudatused tuleb viivitamata edastada kõigile töötajatele, töövõtjatele ja asjakohastele kolmandatele isikutele.

9.4.2 Poliitika ajakohastatud versioonid peavad olema kõigile mõjutatud isikutele kergesti kättesaadavad (nt elektrooniliselt jagatuna või töökohal füüsiliselt välja panduna).

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika on tihedalt seotud organisatsiooni VKE poliitikakomplekti teiste poliitikatega, eelkõige:

10.1.1 P2S – juhtimisrollide ja vastutuste poliitika: täpsustab turbeülesannete ja vastutuste jaotust.

10.1.2 P4S – juurdepääsukontrolli poliitika: määratleb organisatsiooni teabele juurdepääsu turvalise haldamise.

10.1.3 P8S – infoturbe teadlikkuse ja koolituse poliitika: sisaldab töötajate koolituse ja teadlikkuse põhijuhiseid.

10.1.4 P17S – andmekaitse ja privaatsuse poliitika: tagab vastavuse isikuandmete kaitse üldmäärusele ja muudele andmekaitsenõuetele.

10.1.5 P30S – intsidendihalduse poliitika: kirjeldab turvaintsidentidele reageerimiseks vajalikke üksikasjalikke tegevusi.

10.2 Need seotud poliitikad annavad selged tegevusjuhised ja neid tuleb rakendada tervikuna, et saavutada täielik vastavus ISO/IEC 27001 sertifitseerimise nõuetele.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 5.1 – Eestvedamine ja pühendumus: nõuab tippjuhtkonna pühendumust ja vastutust infoturbe tulemuslikkuse eest organisatsioonis.

11.1.2 Punkt 5.2 – Infoturbepoliitika: nõuab selgeid dokumenteeritud poliitikaid, mis on kooskõlas organisatsiooni strateegia ja vastavusnõuetega.

11.1.3 Punkt 5.3 – Organisatsiooni rollid ja vastutused: määratleb infoturbe vastutuste selge jaotuse organisatsioonis, mis on tõhusa juhtimise ja auditite jaoks oluline.

11.1.4 Punkt 6.1 – Riskide ja võimaluste käsitlemise tegevused: tagab, et infoturberiskid tuvastatakse, hinnatakse ja käsitletakse süstemaatiliselt.

11.1.5 Punkt 8.1 – Operatiivne planeerimine ja kontroll: nõuab, et organisatsioon kavandaks ja rakendaks protsessid, mis on vajalikud infoturbe eesmärkide saavutamiseks ja nendega seotud riskide tõhusaks juhtimiseks.

11.2 ISO/IEC 27002:2022 kontrollmeetmed 5.1–5.5

11.2.1 Lisa A kontrollmeede 5.1 – Infoturbepoliitikad: määratleb dokumenteeritud infoturbepoliitikate koostamise ja edastamise.

11.2.2 Lisa A kontrollmeede 5.2 – Infoturbe rollid: täpsustab ja määrab ametlikult infoturbe rollid ja vastutused asjakohastele osapooltele.

11.2.3 Lisa A kontrollmeede 5.3 – Tööülesannete lahusus: nõuab tööülesannete selget lahusust, et vähendada huvide konflikti ja pettuse riski tundliku teabe käitlemisel.

11.2.4 Lisa A kontrollmeede 5.4 – Juhtkonna vastutused: nõuab, et juhtkond näitaks oma pühendumust infoturbele aktiivse järelevalve ja ressursside eraldamise kaudu.

11.2.5 Lisa A kontrollmeede 5.5 – Suhtlemine pädevate asutustega: rõhutab selgelt dokumenteeritud infoturbepoliitikate, rollide, vastutuste ja juhtimisstruktuuride vajalikkust, tagades organisatsioonis järjepideva juhtimise ja auditijälje.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Infoturbeprogrammi plaan: nõuab dokumenteeritud infoturbe juhtimise strateegiaid ja poliitikaid, pakkudes raamistikku järjepidevaks rakendamiseks ja juhtimiseks.

11.3.2 PL-1 – Turbeplaneerimise poliitika: nõuab kogu organisatsiooni hõlmavat turbeplaneerimise poliitikat, mis suunab infoturbe tegevuste turvalist toimimist ja strateegilist kooskõla.

11.3.3 CA-1 – Turbehindamise ja autoriseerimise poliitika: nõuab selgelt määratletud hindamise ja autoriseerimise rolle, et tagada infoturbe nõuete pidev tulemuslikkus ja vastavus.

11.3.4 AC-1 – Juurdepääsukontrolli poliitika: nõuab, et organisatsioon määratleks, dokumenteeriks ja rakendaks selged juurdepääsu haldamise tavad ja vastutused.

11.4 ELi isikuandmete kaitse üldmäärus (2016/679)

11.4.1 Artikkel 5(2) – Vastutuse põhimõte: nõuab, et organisatsioon suudaks tõendada vastavust andmekaitse põhimõtetele, sealhulgas dokumenteeritud rollide ja poliitikate kaudu andmekaitsealaste vastutuste osas.

11.4.2 Artikkel 32 – Töötlemise turvalisus: nõuab asjakohaste tehniliste ja korralduslike meetmete rakendamist, sealhulgas selgete turbevastutuste määramist, et kaitsta isikuandmeid rikkumiste ja volitamata juurdepääsu eest.

11.5 ELi NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(a) – Riskijuhtimismeetmed: nõuab selget juhtimiskorraldust, sealhulgas määratletud rolle ja vastutusi infoturbe valdkonnas, mis on hädavajalikud küberriskide tõhusaks juhtimiseks.

11.6 ELi DORA määrus (2022/2554)

11.6.1 Artikkel 9 – IKT-riskide juhtimine: nõuab, et organisatsioon määraks selgelt IKT-riskide juhtimisega seotud rollid ja vastutused, tugevdades toimepidevust ja talitluspidevuse valmisolekut.

11.6.2 Artikkel 10 – IKT talitluspidevus: nõuab selget vastutust ja struktureeritud rolle IKT toimepidevuse ja vastupidavuse tagamiseks, et organisatsioon saaks häiretele usaldusväärselt reageerida.

11.7 COBIT 2019

11.7.1 EDM03 – Riskide optimeerimise tagamine: rõhutab selgelt määratletud vastutust ja rolle organisatsiooni riskide juhtimisel, toetades tugevat juhtimist ja infoturberiskide tõhusat järelevalvet.

11.7.2 APO13 – Turbe juhtimine: nõuab, et organisatsioon määraks ja teavitaks selgelt turbe juhtimise vastutused, tagades kooskõla ärieesmärkide ja regulatiivsete nõuetega.

11.7.3 DSS05 – Turbeteenuste juhtimine: nõuab struktureeritud rolle ja selgeid vastutusi turbeteenuste juhtimisel, võimaldades järjepidevat rakendamist ja vastavuse kontrolli.