					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P08					Dokumendi pealkiri: **Infoturbeteadlikkuse ja koolituse 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/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 7.3, lisa A kontroll 6.3	Sätestab käesolevas poliitikas käsitletud teadlikkuse ja koolituse nõuded
ISO/IEC 27002:2022	Kontroll 6	Toetab töörollile vastava teadlikkuskoolituse rakendamist
NIST SP 800-53 Rev.5	AT-1 kuni AT-5	On kooskõlas poliitika ja protseduuride, teadlikkuskoolituse, rollipõhise koolituse, koolituskirjete ja turberühmadega suhtlemise nõuetega
ELi isikuandmete kaitse üldmäärus (GDPR)	Artiklid 32, 39; põhjendus 78	Nõuab isikuandmete töötlejate ja töötajate teadlikkuskoolitust
ELi NIS2	Artiklid 21(2)(a, b), 21(3)	Nõuab riskide ja turbekoolituse poliitikaid ning teadlikkuse tõstmise algatusi
ELi DORA	Artiklid 5, 8, 13	Nõuab IKT-riskide teadlikkust ja koolitust toimepidevuse kontrollimeetmete osana
COBIT 2019	APO07, DSS05, MEA	Tugevdab töötajate teadlikkust, kasutajate koolitamist ja vastavuse seiret

1. Eesmärk

1.1 Käesolev poliitika kehtestab formaalse raamistiku, et tagada kõigi töötajate teadlikkus oma infoturbealastest kohustustest ning neile vajaliku koolituse andmine teabevarade konfidentsiaalsuse, tervikluse ja käideldavuse kaitsmiseks.

1.2 See toetab ISO/IEC 27001 punkti 7.3 ja lisa A kontrolli 6.3 nõudeid, kehtestades struktureeritud ja riskipõhise teadlikkuse tõstmise ning koolitusprogrammi, mis on kohandatud organisatsiooni rollidele ja muutuvale ohupildile.

1.3 Poliitika aitab vähendada inimtegurist tulenevaid haavatavusi, edendada turvateadlikku käitumist ja järjepidevalt tugevdada turvalisi tööpraktikaid kooskõlas õiguslike ja lepinguliste nõuetega.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile organisatsiooni infosüsteemidele, andmetele või rajatistele juurdepääsu omavatele sise- ja välistele isikutele, sealhulgas:

2.1.1 töötajad (täistööajaga, osalise tööajaga, ajutised)

2.1.2 töövõtjad, kolmandate osapoolte teenusepakkujad, konsultandid ja praktikandid

2.1.3 kolmandad isikud, kellel on teenuslepingute alusel loogiline või füüsiline juurdepääs

2.2 Kohaldamisala hõlmab:

2.2.1 tööleasumise esmast infoturbeteadlikkuse koolitust

2.2.2 rollipõhist koolitust (nt arendajad, finantstöötajad, privilegeeritud juurdepääsuga kasutajad)

2.2.3 perioodilist täiendkoolitust ja teadlikkuse tõstmise kampaaniaid

2.2.4 ad hoc koolitust vastusena intsidentidele või uutele ohtudele

2.3 Käesoleva poliitika kohaldamisalasse kuuluvad koolituse läbiviimise vormid on e-õpe, kontaktkoolitused, simulatsioonid, teadmiste kontrollid, plakatid, turbeuudiskirjad ja kohustuslikud kinnitused.

3. Eesmärgid

3.1 Tagada, et kõik töötajad mõistavad oma kohustusi organisatsiooni varade kaitsmisel ja turbepoliitikate järgimisel.

3.2 Tagada pidev ja mõõdetav teadlikkuskoolitus, mis on kooskõlas rollipõhise riskiga kokkupuutega.

3.3 Kinnistada turvaline käitumine igapäevastesse tegevustesse, tugevdades selliseid praktikaid nagu paroolide turvaline kasutamine, intsidentidest teatamine ja vastupanu andmepüügile.

3.4 Tagada õigusaktidele vastavus ja auditivalmidus infoturbe koolitusnõuete täitmisel eri tegevusvaldkondades ja jurisdiktsioonides.

3.5 Vähendada hooletusest, teadmatusest või kehvast otsustusest tulenevaid turbeintsidente käitumusliku suunamise ja pideva kinnistamise kaudu.

4. Rollid ja vastutused

4.1 tippjuhtkond

4.1.1 Kinnitab organisatsiooni infoturbe koolitusstrateegia ning tagab selleks vajalike ressursside olemasolu ja lõimimise ettevõtte prioriteetidesse.

4.1.2 Teostab juhtkonna tasandil järelevalvet vastavuse üle ja tagab poliitika järgimise kõigis üksustes.

4.2 infoturbejuht / ISMS-i juht

4.2.1 Vastutab käesoleva poliitika eest ning määratleb teadlikkuse tõstmise ja koolituse raamistiku kooskõlas riskide, vastavusnõuete ja ärivajadustega.

4.2.2 Teostab järelevalvet kõigi turvakoolituse algatuste kavandamise, elluviimise, seire ja läbivaatamise üle.

4.2.3 Tagab koolituste perioodilise ajakohastamise ning nende vastavuse muutuvatele ohtudele ja uutele tehnoloogiatele.

[... 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 ja sellega seotud koolitusprogramm tuleb läbi vaadata:

9.1.1.1 kord aastas või

9.1.1.2 pärast suuremaid inimliku vea või siseohuga seotud intsidente

9.1.1.3 oluliste uute tehnoloogiate või ohtude kasutuselevõtul

9.1.1.4 õiguslike, lepinguliste või sertifitseerimisega seotud kohustuste muutumisel

9.2 läbivaatamise protsess

9.2.1 Läbivaatamist juhib infoturbejuht koordineeritult järgmiste osapooltega:

9.2.1.1 personali- ja koolitusüksused

9.2.1.2 õigus- ja andmekaitse spetsialistid

9.2.1.3 IT-turbe ja operatsiooniriski funktsioonid

9.2.2 Kõik ajakohastused peavad olema:

9.2.2.1 infoturbe juhtimissüsteemi juhtkomitee poolt kinnitatud

9.2.2.2 versioonihalduse all ja dokumenteeritud ISMS-i dokumendiregistris

9.2.2.3 kasutajatele teatavaks tehtud, kui olulised muudatused mõjutavad koolituse kohaldamisala või vastutusi

9.3 sisu ajakohastamise juhtimine

9.3.1 Koolitusmoodulid ja teadlikkuse materjalid tuleb iga 12 kuu järel läbi vaadata, et tagada:

9.3.1.1 asjakohasus ohupildi suhtes

9.3.1.2 regulatiivne täpsus

9.3.1.3 vormingu sobivus (nt juurdepääsetavus, lokaliseerimine)

9.3.2 Aegunud või eksitav sisu tuleb viivitamata kasutuselt kõrvaldada ja asendada heakskiidetud alternatiividega.

10. Seotud poliitikad ja seosed

10.1 Käesolevat poliitikat toetavad ning selle rakendamist toetavad järgmised dokumendid:

10.1.1 P01 – Infoturbepoliitika: kehtestab turvateadlikkuse organisatsiooni ISMS-i ühe põhikontrollimeetmena.

10.1.2 P03 – Lubatud kasutuse poliitika: nõuab koolituse käigus kasutaja kinnitust ja täpsustab igapäevase tehnoloogiakasutusega seotud kohustusi.

10.1.3 P07 – Töölevõtu ja töösuhte lõpetamise poliitika: tagab, et koolitus on lõimitud töösuhte algusesse ja selle läbimist jälgitakse kogu töösuhte jooksul.

10.1.4 P06 – Riskijuhtimise poliitika: seob inimkeskse koolituse ohumudeldamise ja jääkriski vähendamise strateegiatega.

10.1.5 P33 – Auditi ja nõuetele vastavuse seire poliitika: kinnitab auditite käigus, et teadlikkuse kontrollimeetmed on toimivad, mõõdetavad ja tõhusad.

10.2 Koos moodustavad need poliitikad tervikliku käitumuslike kontrollimeetmete raamistiku, mis ühendab teadlikkuse, vastutuse ja kultuurilise kinnistamise.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 7.3 – Teadlikkus: nõuab, et organisatsioon tagaks töötajate teadlikkuse infoturbepoliitikatest ja nende kohustustest. Käesolev poliitika rakendab selle nõude struktureeritud tööleasumise, perioodilise koolituse ja mõõdetava kampaaniates osalemise kaudu.

11.1.2 Lisa A kontroll 6.3 – Infoturbeteadlikkus, haridus ja koolitus: täielikult kaetud esmaste, rollipõhiste ja pidevate koolitusprogrammidega, mis on kohandatud kasutajate riskiprofiilidele.

11.2 ISO/IEC 27002:2022 – Kontroll 6

11.2.1 Toetab töörollile sobiva teadlikkuskoolituse arendamist ja läbiviimist, rõhutades turvalise käitumise kinnistamist ning perioodilisi ajakohastusi ohuteabe ja audititagasiside põhjal.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 kuni AT-5 (teadlikkuse ja koolituse perekond): käesolev poliitika on kooskõlas kontrollidega AT-1 (poliitika ja protseduurid), AT-2 (teadlikkuskoolitus), AT-3 (rollipõhine koolitus), AT-4 (turvakoolituse kirjed) ja AT-5 (kontakt turberühmadega).

11.3.2 IA-5, AC-2: tugevdavad kasutajate vastutust turvalise autentimise ja lubatud kasutuse eest, mis on teadlikkusprogrammide käitumuslike tulemuste keskmes.

11.3.3 IR-1 kuni IR-8: valmidust intsidendihalduseks tugevdatakse sihipäraste teadlikkuskampaaniate ja simulatsioonide kaudu.

11.4 ELi isikuandmete kaitse üldmäärus (2016/679)

11.4.1 Artikkel 32 – töötlemise turvalisus: nõuab, et isikuandmeid töötlevad töötajad oleksid koolitatud isikuandmetega seotud riskide tuvastamiseks, ennetamiseks ja neist teatamiseks. Käesolev poliitika tagab vastava koolituse andmise isikuandmete töötlejatele ja kõigile teistele asjakohastele rollidele.

11.4.2 Artikkel 39 – andmekaitsespetsialisti ülesanded: hõlmab teadlikkuse tõstmist ja töötlemistoimingutes osalevate töötajate koolitamist.

11.4.3 Põhjendus 78: soodustab asjakohaseid teadlikkusmeetmeid, et tagada tugevad turvapraktikad ja poliitika järgimine.

11.5 ELi NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(a, b): nõuab, et üksused võtaksid vastu riskianalüüsi ja turbekoolituse poliitikad kõigile asjakohastele töötajatele. Käesolev poliitika täidab selle nõude, kehtestades pidevad ja rollitundlikud koolitusprotsessid.

11.5.2 Artikkel 21(3): soodustab küberturbe riskiteadlikkuse edendamist juhtkonna ja töötajate seas teadlikkuse algatuste ja simulatsioonide kaudu.

11.6 ELi DORA (2022/2554)

11.6.1 Artikkel 13 – digitaalne operatiivse toimepidevuse strateegia: nõuab, et IKT-riskide teadlikkus ja koolitus oleksid osa juhtimismudelist. Käesolev poliitika tagab inimriskide käsitlemise pideva koolituse ja ohusimulatsioonide kaudu.

11.6.2 Artiklid 5 ja 8: rõhutavad sisekontrolli raamistike olulisust, milles teadlikkus ja koolitus on IKT toimepidevuse ning küberhügieeni põhikomponendid.

11.7 COBIT 2019

11.7.1 APO07 – juhitud personalijuhtimine: rõhutab vajadust arendada teadlikkust turbekohustustest ja lõimida see tööjõu juhtimisse.

11.7.2 DSS05 – juhitud turvateenused: kehtestab kontrollimeetmed kasutajate koolituse ja intsidentidest teatamise üle, mis mõlemad on käesoleva poliitika lahutamatud osad.

11.7.3 MEA03 – vastavuse seire, hindamine ja auditeerimine: nõuab kasutajakäitumise ja poliitika järgimise tõhususe läbivaatamist, mida rakendatakse siin andmepüügitestide, testide ja teadlikkuskampaaniate mõõdikute kaudu.