					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P08S					Dokumendi pealkiri: **Infoturbe teadlikkuse 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 õigusnormidega

Standard/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 7	
ISO/IEC 27002:2022	Kontroll 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
ELi NIS2	Artikkel 21(2)(i)	
ELi DORA	Artikkel 13	
COBIT 2019	BAI08, DSS	
ELi isikuandmete kaitse üldmäärus (GDPR)	Artikkel 32, 39	

1. Eesmärk

1.1. Käesoleva poliitika eesmärk on tagada, et kõik töötajad ja töövõtjad mõistavad oma infoturbega seotud kohustusi.

1.2. Poliitika eesmärk on vähendada inimlike eksimuste tõenäosust, parandada võimet intsidente tuvastada ja neist teatada ning kujundada kogu organisatsioonis infoturbeteadlikku kultuuri.

1.3. Poliitika toetab vastavust standarditele ISO/IEC 27001, NIS2, GDPR ja DORA, lõimides infoturbeteadlikkuse igapäevasesse töökäitumisse ja rollipõhistesse ootustesse.

2. Kohaldamisala

2.1. Käesolev poliitika kehtib kõigile töötajatele, töövõtjatele, praktikantidele ja kolmandatele isikutele, kellel on juurdepääs ettevõtte süsteemidele või andmetele.

2.2. See hõlmab järgmist:

2.2.1. tööle asumisel läbiviidav infoturbeteadlikkuse algkoolitus uuele personalile

2.2.2. iga-aastane infoturbeteemaline korduskoolitus

2.2.3. sündmuspõhised teadlikkuse tõstmise tegevused (nt intsidendiga seotud teavitused, plakatid või soovitused)

2.3. Poliitika kehtib kõigis ametikohtades, osakondades ja töökohtades.

3. Eesmärgid

3.1. Tagada, et kogu personal saab õigeaegset, arusaadavat ja asjakohast infoturbeteadlikkuse alast koolitust.

3.2. Anda töötajatele võimekus tuvastada ja vältida levinud ohte, nagu andmepüük, pahavara ja andmelekked.

3.3. Tagada koolituse läbimise dokumenteerimine, et tõendada vastavust õiguslikele, lepingulistele ja auditinõuetele.

3.4. Hoida koolituse sisu ajakohasena, et see kajastaks organisatsiooni poliitikaid, ohte ja kohaldatavaid õigusnorme.

3.5. Kujundada töötajates ennetav hoiak, mille kohaselt infoturve on igapäevase vastutuse osa.

4. Rollid ja vastutused

4.1. Tegevjuht

4.1.1. Kiidab heaks koolitusnõuded ja tagab vajalike ressursside eraldamise.

4.1.2. Vaatab läbi koolituse läbimise aruanded ja eskaleerib mittevastavused vajaduse korral.

4.2. Büroojuht / personalijuhtimine (HR)

4.2.1. Koordineerib uute töötajate koolituste korraldamist ja iga-aastase korduskoolituse läbiviimist.

4.2.2. Haldab koolituskirjeid ja koolitusloge.

4.2.3. Tagab, et töötajad kinnitavad tutvumist peamiste infoturbepoliitikate ja konfidentsiaalsuslepinguga (NDA).

[... 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. Käesoleva poliitika vaatavad tegevjuht ja personalijuhtimine (HR) läbi kord aastas, et tagada selle vastavus kehtivatele riskidele, õigusnormidele ja tööjõu vajadustele.

9.2. Vahepealsed ajakohastused

9.2.1. Poliitika ja koolituse sisu tuleb samuti läbi vaadata ja ajakohastada pärast järgmist:

9.2.1.1. olulist turbeintsidenti

9.2.1.2. õiguslikke või lepingulisi muudatusi

9.2.1.3. organisatsioonilisi ümberkorraldusi või süsteemide migreerimist

9.3. Versioonihaldus ja levitamine

9.3.1. Iga ajakohastus peab sisaldama järgmist:

9.3.1.1. versiooninumber ja jõustumiskuupäev

9.3.1.2. muudatuste kokkuvõte

9.3.1.3. tegevjuhi heakskiit

9.3.1.4. kõigi varasemate versioonide arhiiv, mida säilitatakse vähemalt kolm aastat

9.4. Töötajate teavitamine

9.4.1. Poliitika ajakohastused tuleb edastada kõigile töötajatele ning oluliste muudatuste korral tuleb saada tutvumiskinnitus.

10. Seotud poliitikad ja seosed

10.1. Käesolev poliitika toetab järgmisi dokumente:

10.1.1. P2S – Juhtimisrollide ja vastutuste poliitika: määrab koolituse koordineerimise ja järelevalve vastutuse

10.1.2. P3S – Lubatud kasutuse poliitika: kinnistab koolitusel käsitletud käitumisootusi

10.1.3. P4S – Juurdepääsukontrolli poliitika: tagab, et kasutajad mõistavad juurdepääsu turvalisuse tähtsust

10.1.4. P7S – Töölevõtmise ja töösuhte lõpetamise poliitika: lõimib koolituse tööle asumise protsessi

10.1.5. P30S – Intsidentidele reageerimise poliitika: tagab, et töötajad oskavad intsidentidest kiiresti ja korrektselt teatada

11. Viitestandardid ja raamistikud

11.1. ISO/IEC 27001

11.1.1. Punkt 7.3 – nõuab, et organisatsioon tagaks personali teadlikkuse oma kohustustest ja infoturbe mõjust

11.2. ISO/IEC 27002

11.2.1. Kontroll 6.3 – kirjeldab ootusi infoturbeteadlikkuse koolituse ulatusele ja läbiviimisele

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – nõuab teadlikkuse alast koolitust kasutajatele, kellel on süsteemidele juurdepääs

11.3.2. AT-4 – käsitleb rollipõhist koolitust ja mittevastavuse tagajärgi

11.4. ELi isikuandmete kaitse üldmäärus (GDPR)

11.4.1. Artikkel 32 – nõuab turvameetmeid, sealhulgas personali koolitamist, et kaitsta isikuandmeid

11.4.2. Artikkel 39 – nõuab andmekaitseametnikult teadlikkuse ja koolituse järelevalvet, kui see on asjakohane

11.5. ELi NIS2 direktiiv

11.5.1. Artikkel 21(2)(i) – nõuab pidevaid küberturvalisuse teadlikkuse tõstmise ja koolituse programme

11.6. ELi DORA

11.6.1. Artikkel 13 – nõuab, et finantssektori üksused rakendaksid väljaõpet ja koolitust kõigile töötajatele, kellel on IKT-ga seotud kohustused

11.7. COBIT 2019

11.7.1. BAI08 – teadmushaldus: tagab, et töötajad on pädevad ja koolitatud

11.7.2. DSS05 – turvateenuste haldamine: rõhutab teadlikkust kui olulist kaitsemeedet