Promens Rõngu AS

# INFOTURBEPOLIITIKA

Põhimõtted infoturbe süsteemi korraldamiseks

# 1 Dokumendi versioonikontroll

| | Viimati muudetud | Viimati muutnud | Dokumendi muudatused |
|---|---|---|---|
| 0.1 | 09.04.2024 | JE | Esimesena loodud dokument |
| 0.2 | 8.08.2024 | JE | TLP muudetud - “Ettevõttesisene kasutus” asemel “Avalik dokument” |
| | | | |

# 2 Dokumendi sisu lehekülg

# 3 Infoturbepoliitika

## 3.1 Eesmärk

Käesoleva poliitika eesmärk on sätestada organisatsiooni suhtes kohaldatavad infoturbepõhimõtted, et kaitsta andmete konfidentsiaalsust, terviklikkust ja kättesaadavust.

## 3.2 Reguleerimisala

Kõik töötajad ja kolmandatest isikutest kasutajad.

## 3.3 Põhimõte

Infoturbe haldamine põhineb riskil, õiguslikel ja regulatiivsetel nõuetel ning ärivajadusel.

Informatsiooni terviklus, käideldavus ja konfidentsiaalsus tuleb tagada ulatuses, mis võimaldab ettevõttel tõenäolisemate ohtude realiseerumisel häireteta oma ülesandeid täita.

Turvameetmed peavad olema majanduslikult õigustatud ja proportsioonis võimaliku kahjuga, mis võib tekkida meetmete puudulikkuse tõttu ning nende häiriv toime ettevõtte tegevusele ja töötajate tööle peab olema võimalikult väike.

## 3.4 Tegevjuhi kohustuste deklaratsioon

“Ettevõttena on teabe töötlemine meie edu aluseks ning selle teabe kaitse ja turvalisus on juhtkonna tasandil prioriteet. Olenemata sellest, kas tegemist on töötajate või klientide teabega, võtame oma kohustusi, mis tulenevad GDPRist, kliendinõuetest ja andmekaitseseadusest, väga tõsiselt. Oleme eraldanud ressursse, et arendada, rakendada ja pidevalt täiustada meie äritegevusele sobivat infoturbe haldamist."

*ÜS, tegevjuht, 3.05.2024*

## 3.5 Sissejuhatus

Infoturve kaitseb meile usaldatud teavet. Kui infoturve ei toimi nõuetekohaselt, võib see avaldada märkimisväärset kahjulikku mõju meie töötajatele, klientidele, mainele ja finantstulemustele. Kui meil on tõhus infoturbe haldussüsteem, saame me

- Anda tagatisi meie kliendinõuete, õiguslike, regulatiivsete ja lepinguliste kohustuste täitmiseks.
- Tagada, et õigetel inimestel on õige juurdepääs õigetele andmetele õigel ajal.
- Tagada isikuandmete kaitse vastavalt GDPRi määratlusele.
- Olge head andmekogujad ja -hoidjad.

## 3.6 Infoturbe eesmärgid

Tagada organisatsiooni teabe, sealhulgas kõigi isikuandmete konfidentsiaalsus, terviklikkus ja kättesaadavus, nagu on määratletud GDPRis ja kliendinõuetes, lähtudes heast riskijuhtimisest, õiguslikest regulatiivsetest ja lepingulistest kohustustest ning ärivajadustest.

Tagada infoturbe haldamise süsteemi väljatöötamiseks, rakendamiseks ja pidevaks täiustamiseks vajalikud ressursid.

Tõhusalt hallata kolmanda osapoole tarnijaid, kes töötlevad, salvestavad või edastavad teavet, et vähendada ja hallata infoturvariske.

Rakendada infoturbe- ja andmekaitsekultuuri tõhusa koolituse ja teadlikkuse tõstmise kaudu.

## 3.7 Infoturbe määratlus

Infoturve on defineeritud kui säilitamine

| | |
|---|---|
| **Konfidentsiaalsus (Confidentiality)** | Juurdepääs teabele on neil, kellel on asjakohased volitused<br><br>***Õiged inimesed õigete juurdepääsudega*** |
| **Terviklikkus (Integrity)** | teave on täielik ja täpne<br><br>***õigetele andmetele*** |
| **Kättesaadavus (Availability)** | Teave on kättesaadav siis, kui seda vajatakse<br><br>***õigel ajal ja õiges kohas*** |

## 3.8 Infoturbepoliitika raamistik

Infoturbe haldamise süsteem põhineb infoturbepoliitika raamistikul. Koos selle poliitikaga moodustavad poliitikaraamistiku järgmised poliitikad:

- DP 01 **Andmekaitsepoliitika**
- DP 02 **Andmete säilitamise poliitika**
- IS 01 **Infoturbepoliitika** (käesolev poliitika)
- IS 02 **Juurdepääsukontrolli poliitika**
- IS 03 **Varade haldamise poliitika**
- IS 04 **Riskijuhtimise poliitika**
- IS 05 **Teabe klassifitseerimise ja käitlemise poliitika**
- IS 06 **Infoturbealase teadlikkuse ja koolituse poliitika**
- IS 07 **Infovarade aktsepteeritava kasutamise poliitika**
- IS 08 **Tühja töölaua ja Tühja ekraani poliitika**
- IS 09 **Mobiilse ja kaugtöö poliitika**
- IS 10 **Äritegevuse jätkusuutlikkuse poliitika**
- IS 11 **Varunduse poliitika**
- IS 12 **Pahavara- ja viirusetõrje poliitika**
- IS 13 **Muudatuste juhtimise poliitika**
- IS 14 **Tarnijate ja kolmandate osapoolte turvapoliitika**
- IS 15 **Pideva parendamise poliitika**
- IS 16 **Logimise ja järelevalve poliitika**
- IS 17 **Võrgu turvalisuse juhtimise poliitika**

- IS 18 **Teabevahetuse poliitika**
- IS 19 **Turvalise arenduse poliitika**
- IS 20 **Füüsilise keskkonna turvalisuse poliitika**
- IS 21 **Krüptograafiliste võtmete haldamise poliitika**
- IS 22 **Krüptograafilise kontrolli ja krüpteerimise poliitika**
- IS 23 **Dokumentide ja registrite poliitika**
- IS 24 **Oluliste vahejuhtumite ja tõendite kogumise poliitika**
- IS 25 **Tarkvara paranduste poliitika**
- IS 26 **Pilveteenuste poliitika**
- IS 27 **Intellektuaalomandi õiguste poliitika**

## 3.9 Infoturbe rollid ja kohustused

Infoturve on igaühe kohustus mõista ja järgida poliitikaid, järgida menetlusi ja teatada kahtlustatavatest või tegelikest rikkumistest. Konkreetsed rollid ja vastutusalad infoturbe haldamise süsteemi toimimiseks on määratletud ja dokumenteeritud dokumendis "**Infoturbe rollide määramine ja kohustused".**

## 3.10 Järelevalve

Infoturbe haldamise süsteemi põhimõtete ja teostuse järgimist jälgib juhtkond koos sise- ja välisauditi poolt perioodiliselt teostatavate sõltumatute ülevaatustega.

## 3.11 Õiguslikud ja regulatiivsed kohustused

Organisatsioon võtab oma õiguslikke ja regulatiivseid kohustusi tõsiselt ning need nõuded on registreeritud dokumendis "**V2.6.2 Kliendinõuete maatriks"** ja **“Dokumentide register PETKAs -> normatiivaktid”**

## 3.12 Koolitus ja teadlikkuse tõstmine

Poliitikad tehakse kõigile töötajatele ja kolmandatele osapooltele kergesti ja lihtsalt kättesaadavaks. Kehtestatud on koolitus- ja teabevahetuskava, et teavitada infoturbe põhimõtetest, protsessidest ja kontseptsioonidest. Koolitusvajadused on kindlaks määratud ja asjakohased koolitusnõuded on defineeritud "**Kompetentsimaatriksis PETKAs”**.

## 3.13 Juhtimissüsteemi pidev parendamine

Infoturbe haldamise süsteemi täiustatakse pidevalt. **Pideva parendamise poliitika** sätestab ettevõtte lähenemisviisi pidevale parendamisele ja igas protsessis on olemas pideva parendamise osa.

# 4 Poliitika järgimine

## 4.1 Vastavuse mõõtmine

Infoturbe juhtimisrühm kontrollib selle poliitika järgimist erinevate meetodite abil, sealhulgas, kuid mitte ainult, ärivahendite aruannete, sise- ja välisauditite ning poliitika omanikule antava tagasiside abil.

## 4.2 Erandid

Kõik erandid poliitikast peab eelnevalt heaks kiitma ja registreerima infoturbejuht ning teatama sellest juhtkonda.

## 4.3 Nõuetele mittevastavus

Töötaja suhtes, kelle puhul leitakse, et ta on seda poliitikat rikkunud, võidakse rakendada distsiplinaarmeetmeid kuni töösuhte lõpetamiseni.

## 4.4 Poliitika ajakohastamine

Poliitikat ajakohastatakse ja vaadatakse läbi pideva parendusprotsessi raames.

# 5 ISO27001 standardi käsitletavad valdkonnad

ISO27001-le vastav teabeturbepoliitika

| ISO27001:2022 | ISO27002:2022 |
|---|---|
| ISO27001:2022 punkt 5 Juhtimine | ISO27002:2022 punkt 5 Organisatsiooniline kontroll |
| ISO27001:2022 punkt 5.1 Juhtimine ja pühendumine | ISO27002:2022 punkt 5.1 Infoturbe põhimõtted |
| ISO27001:2022 punkt 5.2 Poliitika | ISO27002:2022 punkt 5.36 Vastavus infoturbe põhimõtetele, eeskirjadele ja standarditele |
| ISO27001:2022 punkt 6.2 Infoturbe eesmärgid ja nende saavutamise planeerimine | ISO27002:2022 punkt 5.4 Juhtkonna kohustused |
| ISO27001:2022 punkt 7.3 Teadlikkus | ISO27002:2022 punkt 6 Inimeste kontroll |
| | ISO27002:2022 punkt 6.3 Infoturbealase teadlikkuse tõstmine, haridus ja koolitus |
| | ISO27002:2022 Klausel 6.4 Distsiplinaarmenetlus |