# OIXIO Cyber

## Eesti uus Küberturvalisuse seadus (KüTS) – vastavus ja rakendamine

TRINITI
TALLINN RIGA VILNIUS

oixio.eu

## Euroopa Liidu NIS2 direktiivi ülevõtmine

**2023. aasta jaanuar** → **2026. aasta jaanuar** → **Kuni 31.03.2026** → **Kuni 3 aastat**

NIS2 direktiiv hakkas EL-s kehtima

NIS2 võeti üle KüTS-i

AEGA TEAVITAMISEKS
Täitke avaldus: eesti.ee

AEGA VASTAVUSE TAGAMISEKS

## Kellele uus seadus kohaldub?

KüTS kohaldub ligikaudu 6500 ettevõttele ja asutusele Eestis.
Seadus jaotab ettevõtted kahte kategooriasse:

### Üliolulised üksused

Kriitilise tähtsusega teenusepakkujad, kelle häired mõjutavad otsustavalt ühiskonna toimimist ja julgeolekut. Rangemad nõuded ja suuremad sanktsioonid.

Teatud kategooriad on suurusest sõltumatud.
Reegel: **vähemalt 250 töötajat**
**+ aasta bilansimaht ületab 43 miljonit €**
**või aastakäive ületab 50 miljonit €.**

### Olulised üksused

Oluliste teenuste pakkujad, kelle häired võivad mõjutada teenuste osutamist. Kohalduvad küberturvalisuse põhinõuded.

Reegel: **vähemalt 50 töötajat**
**+ aasta bilansimaht**
**või aastakäive on rohkem kui 10 miljoni €.**

## Mis täpsemalt muutus?

- **Subjektide ringi laienemine.** Lisandus ~3000 uut organisatsiooni (kokku ~6500)
- **Juhtkonna vastutus.** Juhtorganil on otsene kohustus ja vastutus küberturbe eest
- **Koolituskohustus.** Regulaarne küberturvalisuse alane koolitus juhtkonnale ja personalile
- **Tarneahela turvalisus.** Kohustus hinnata ja jälgida partnerite küberturvet
- **Intsidentide raporteerimise nõuded.** Kohustuslik ja kiire teavitamine pädevatele asutustele (CERT-EE, RIA)
- **Riskijuhtimise raamistik.** Kohustuslik küberturvalisuse riskide hindamine ja juhtimine
- **Auditikohustus.** Sõltuvalt kategooriast kohustuslik või soovitatav audit
- **Dokumentatsioonikohustus.** Põhjalik dokumentatsioon ja selle ajakohasus

## Millised on sanktsioonid?

Mittevastavuse korral kohaldatakse märkimisväärseid sanktsioone:

TRAHV üliolulistele üksustele
**kuni 10 miljonit €**
või 2% ülemaailmsest aastakäibest (kõrgem kahest)

TRAHV olulistele üksustele
**kuni 7 miljonit €**
või 1,4% ülemaailmsest aastakäibest (kõrgem kahest)

Küberturvalisuse eest vastutava juhatuse liikme isiklik vastutus

### Sektoripõhine kohaldamine

Alljärgnevad sektorid kuuluvad seaduse kohaldamisalasse:

- energia
- reovesi
- posti- ja kullerteenused
- transport
- digitaalne infrastruktuur
- jäätmekäitlus
- pangandus
- IKT teenused (B2B)
- kemikaalide tootmine
- finantsturg
- avalik haldus
- toidu tootmine
- tervishoid
- kosmos
- teadusuuringud
- joogivesi

# 10 põhilist sammu KüTS rakendamiseks

Praktiline tegevuskava vastavuse saavutamiseks (koostöös Advokaadibürooga TRINITI)

### 1 Tee kindlaks, kas olete KüTS kohuslane

Esimese asjana tuleb teha kindlaks, kas organisatsioon kuulub ülioluliste või oluliste üksuste hulka vastavalt Eesti küberturvalisuse seadusele. Samuti tuleb välja selgitada võimalik auditi kohustus. NB! Kõik KüTS subjektid peavad end ise RIA-le "üles andma" kolme kuu jooksul. Selleks logi sisse juriidilise kontoga eesti.ee portaali ja täida asjakohane vorm.

*TRINITI aitab - konsultatsioon*

### 2 Vastutuse ja delegeerimise otsus

KüTS paneb rõhku ka tarneahelale, kelle eest lõppvastutus jääb siiski organisatsioonile endale. Kui kaasad teenusepakkujaid, siis on oluline, et ka nemad rakendavad turvameetmeid. Hoolitse, et lepingud on korras.

*TRINITI aitab - nõustamine ja lepingute koostamine*

### 3 Juhtkonna vastutus ja rollide määramine

Juhtkond peab kinnitama oma küberturbe alase pühendumuse ja vastutuse. Vajadusel tuleb määrata infoturbejuht ning kehtestada üldine infoturbe alane vastutus ja rollid. Dokumenteerige vastutusalad. Kehtestage aruandluse kord juhtkonnale. Otsustage, kas valite ISMS aluseks ISO 27001 või E-ITS standardi.

*OIXIO Cyber aitab - konsultatsioon või Infoturbejuht teenusena (vCISO)*

### 4 Äriprotsesside kaardistamine ja olukorra hindamine

Kaardistage äriprotsessid ja infovarad ning määrake nende eest vastutajad. Teostage olemasoleva küberturbe olukorra hindamine. Soovitatav on tellida küberturbe olukorra hindamine väliselt osapoolelt, kes annab objektiivse hinnangu ettevõtte seisule. Hindamise tulemus on hea sisend edasistele tegevustele.

*OIXIO Cyber aitab - KüTS vastavushindamise teenus või küberturbeaudit*

### 5 Riskianalüüs ja riskijuhtimise raamistik

Valige riskianalüüsi meetoodika ning teostage riskianalüüs. Riskianalüüsis tuleb arvestada küberohtudega, füüsiliste ohtudega ning tarneahela riskidega. Riskianalüüsi tulemusena tekib riskide käsitlemise plaan. Samuti tuleb kinnitada organisatsiooni riskitaluvuse määr ning jääkriskid.

*OIXIO Cyber aitab - konsultatsioon või Infoturbejuht teenusena (vCISO)*

### 6 Infoturbemeetmete rakendamise plaan

Koostage infoturbemeetmete rakendamise plaan. Plaan peab minimaalselt sisaldama meetmete rakendamise tähtaegu ning vastutajaid, samuti iga meetme rakendamise olekut. Dokumenteerida tuleb ka, kuidas iga meede on organisatsioonis rakendatud. See on teie tegevuskava vastavuse saavutamiseks.

*OIXIO Cyber aitab: Konsultatsioon või Infoturbejuht teenusena (vCISO)*

### 7 Dokumentatsiooni loomine

Looge vajalik dokumentatsioon. Koostada tuleb infoturvapoliitika ja infoturbe strateegia. Lisaks tuleb luua valdkondlikud poliitikad ja protseduurid. Dokumentatsioon peab olema ajakohane, ligipääsetav ja vastama valitud standardile (ISO 27001 või E-ITS).

*OIXIO Cyber aitab: Konsultatsioon või Infoturbejuht teenusena (vCISO)*

### 8 Intsidentide halduse ja raporteerimise süsteem

Koostage küberintsidentide halduse raporteerimise poliitikad ja protseduurid. Juurutage turvameetmed ja tehnoloogiad, mis tagavad küberintsidentideks valmisoleku. Määratlege selged protsessid intsidentide tuvastamiseks, reageerimiseks ja CERT-EE/RIA-le teavitamiseks.

*OIXIO Cyber aitab: Küberturbe Keskus teenusena (SOCaaS) - 24/7 monitooring ja intsidendihaldus*

### 9 Küberteadlikkuse programm ja koolitus

Looge küberturbe teadlikkuse tõstmise programm, mis hõlmab kogu organisatsiooni. Viige läbi regulaarseid küberturbealaseid koolitusi. Oluline on meeles pidada, et infoturbe eest vastutvatele juhtkonna liikmetele kehtib koolituskohustus. Teadlikud töötajad on parim kaitse.

*OIXIO Cyber aitab - küberhügieeni koolitus, õngitsusrünnakute matkimine (Phishing Simulation), kriisiõppus*

### 10 Pidev parendamine ja kontroll

Tegelege infoturbe juhtimise süsteemi pideva parendamisega ning kontrolliga. Infoturbejuhtimise süsteemi juurutamine ei ole ühekordne tegevus, vaid vajab pidevat tähelepanu. Infoturbemeetmete rakendamist tuleb pidevalt kontrollida ja dokumentatsiooni ning riskianalüüsi uuendada.

*OIXIO Cyber aitab - konsultatsioon või infoturbejuht teenusena (vCISO) - pidev tugi ja järelvalve*

## Sa ei ole uute kohustustega üksi. Oleme alati olemas, küsi julgesti:


**Kristena Kutti**
TRINITI Advokaadibüroo
kristena.kutti@triniti.ee

**Jaan Sõsun**
jaan.sosun@oixio.eu
+372 5560 7898

**Erki Markus**
erki.markus@oixio.eu
+372 520 1293


**OIXIO Cyber terviklik lähenemine tagab:**

Vastavus ei jää pelgalt "linnukeseks kontrollnimekirjas", vaid muutub praktiliseks, toimivaks ja auditeeritavaks süsteemiks, mis kaitseb äritegevust ka reaalsete küberrünnete korral.


KÕRGE
KLIENDIRAHULOLUGA ETTEVÕTE

cyber@oixio.eu; +372 699 0690

OIXIO IT on kõrgeima kliendirahuloluga IT-ettevõte Eestis.
Allikas: *Recommy.com*