| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sisestage siia registreeritud juriidilise isiku nimi | | | | | | | |
| Dokumendi number:<br>P21S | | | | | Dokumendi pealkiri:<br>**Võrguturbe poliitika** | | | | | | | |
| Versioon:<br>1.0 | | Jõustumiskuupäev:<br>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 8 | - |
| ISO/IEC 27002:2022 | Kontroll 8 | - |
| NIST SP 800-53 Rev.5 | AC-4, SC-7 | - |
| ELi GDPR | Artikkel 32 | - |
| ELi NIS2 | Artiklid 21(2)(d), (e) | - |
| ELi DORA | Artiklid 9, 10 | - |
| COBIT 2019 | DSS05.02, APO13 | - |

**1. Eesmärk**

1.1. Käesoleva poliitika eesmärk on tagada, et kogu sisemine ja väline võrgusuhtlus on selgelt määratletud turbekontrollidega kaitstud loata juurdepääsu, rikkumise, pealtkuulamise ja väärkasutuse eest.

1.2. Poliitika kehtestab nõuded võrgutaristu turvaliseks kavandamiseks, kasutamiseks ja haldamiseks, sealhulgas ruuterite, traadita pääsupunktide, kaugjuurdepääsuühenduste ja segmenteeritud võrkude puhul.

1.3. Poliitika eesmärk on minimeerida internetipõhiste ohtude mõju, tagada sise- ja välisvõrkudes edastatavate andmete konfidentsiaalsus ning säilitada kriitiliste teenuste käideldavus.

1.4. Käesolev poliitika toetab ISO/IEC 27001:2022 sertifitseerimist ning aitab otseselt täita GDPR-ist, NIS2-st ja DORA-st tulenevaid õiguslikke ja regulatiivseid kohustusi, pakkudes samal ajal tehnilist kindlust klientidele ja audiitoritele.

**2. Kohaldamisala**

**2.1. Käesolev poliitika kohaldub organisatsiooni IT-võrgu kõigile komponentidele, sealhulgas:**

2.1.1. kontorites kasutatav traadiga ja traadita taristu

2.1.2. ruuterid, kommutaatorid, pääsupunktid, tulemüürid ja lüüsid

2.1.3. kaugjuurdepääsuühendused, sealhulgas VPN-id, RDP ja pilvetunnelid

2.1.4. pilvepõhised rakendused, millele pääsetakse ligi sise- või välisvõrkudest

2.1.5. seadmed, mille töötajad, töövõtjad või külalised ühendavad võrku

2.2. Käesolev poliitika reguleerib nii füüsilisi kui ka loogilisi võrgusegmente, sealhulgas külalisvõrke, asjade interneti (IoT) seadmeid ja taustsüsteeme.

**2.3. Poliitika hõlmab kõiki isikuid, kellel on juurdepääs organisatsiooni võrgule, sealhulgas:**

2.3.1. töötajad

2.3.2. kaugtöötajad ja hübriidtöötajad

2.3.3. välised tarnijad, konsultandid ja teenuseosutajad

2.3.4. külalised, kes kasutavad ajutist Wi-Fi-juurdepääsu

**3. Eesmärgid**

3.1. Tagada, et organisatsiooni võrk on kaitstud loata juurdepääsu ja väliste küberohtude eest

3.2. Rakendada asjakohane segmenteerimine usaldatud ja mitteusaldatud võrkude vahel (nt külaliste Wi-Fi, tarnijate juurdepääs)

3.3. Võimaldada turvaline kaugühendus sisemisi süsteeme ohtu seadmata

3.4. Tõkestada pahavara levikut ja andmete väljaviimist võrgukanalite kaudu

3.5. Tagada võrgutegevuse seire, teavitamine ja auditilogimine intsidendituvastuse ja vastavuse toetamiseks

3.6. Tagada, et sisevõrkudega saavad ühenduda ainult heakskiidetud ja kaitstud seadmed

3.7. Täita ISO 27001-st, GDPR-ist ja seotud küberturbe raamistikest tulenevad kohustused

**4. Rollid ja vastutused**

**4.1. Tegevjuht (GM)**

4.1.1. Vastutab käesoleva poliitika eest ja tagab, et turvaliseks võrgu kavandamiseks ning haldamiseks on eraldatud asjakohased ressursid

4.1.2. Vaatab läbi võrgu turbekontrollide erandid ja kiidab heaks tarnijate võrgujuurdepääsu kokkulepped

4.1.3. Vaatab läbi intsidendid või auditileiud, mis on seotud võrgu turbenõrkustega

**4.2. IT-toe teenuseosutaja / sisemine IT-vastutaja**

4.2.1. Rakendab, seadistab ja haldab kõiki tulemüüre, ruutereid, kommutaatoreid ja traadita võrgu kontrollereid

4.2.2. Haldab sisevõrkude, külalisvõrkude ja välisvõrkude vahelist segmenteerimist

4.2.3. Seirab logisid ja automaatseid teavitusi loata juurdepääsukatsete või võrgus esinevate anomaaliate tuvastamiseks

4.2.4. Tagab, et püsivara- ja konfiguratsioonivärskendused rakendatakse turvaliselt ja õigeaegselt

[ ... 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 peab vähemalt kord aastas läbi vaatama tegevjuht koos IT-toe teenuseosutaja ja andmekaitsekoordinaatoriga

**9.2. Vahepealse läbivaatamise alused**

**9.2.1. Poliitika läbivaatamine tuleb algatada ka järgmistel juhtudel:**

9.2.1.1. olulised muudatused võrguarhitektuuris (nt uued VPN- või tulemüürisüsteemid)

9.2.1.2. võrguga seotud intsident (nt sissetung, lunavara levik või andmete väljaviimine)

9.2.1.3. võrgu kaitset mõjutavad õiguslikud, regulatiivsed või raamistikest tulenevad muudatused

9.2.1.4. uued tarnijaplatvormid, mis nõuavad alternatiivseid juurdepääsumeetodeid või protokolle

**9.3. Versioonihaldus ja dokumentatsioon**

9.3.1. Poliitika muudatused tuleb registreerida versiooninumbri, kuupäeva ja muudatuste kokkuvõttega

9.3.2. Varasemaid versioone tuleb arhiveerida vähemalt 3 aastat

9.3.3. Muudatustest tuleb mõjutatud töötajaid teavitada ning oluliste käitumisreeglite muutmise korral tuleb neilt võtta kinnitus

**10. Seotud poliitikad ja seosed**

**10.1. Käesolevat poliitikat tuleb rakendada koos järgmiste VKE infoturbepoliitikatega:**

10.1.1. P9S – kaugtööpoliitika: sätestab turvalised kaugjuurdepääsuviisid, VPN-i nõuded ja lõppseadmete kaitse nõuded väljaspool ettevõtte asukohti töötavatele kasutajatele.

10.1.2. P12S – varahalduse poliitika: tagab, et kõik võrku ühendatud süsteemid on tuvastatud, kategoriseeritud ja jälgitud koos ajakohase turbestaatusega.

10.1.3. P17S – andmekaitse ja privaatsuse poliitika: tagab, et võrgu segmenteerimine, juurdepääsukontroll ja logimine toetavad GDPR-ist tulenevaid privaatsuse ja andmekaitse põhimõtteid.

10.1.4. P22S – logimis- ja seirepoliitika: määrab nõuded logide kogumiseks ja läbivaatamiseks võrguseadmetest, kaugühendustest ja traadita võrgu kontrolleritest.

10.1.5. P30S – intsidentidele reageerimise poliitika: määratleb nõutavad tegevused võrgu rikkumiste, loata juurdepääsukatsete või sisevõrkude kaudu toimuva pahavara leviku korral.

## 11. Viitestandardid ja raamistikud

### 11.1. ISO/IEC 27001

11.1.1. Punkt 8.1 – nõuab kontrollimeetmete rakendamist turvaliste ja toimepidevate operatsioonide, sealhulgas võrkude tagamiseks.

### 11.2. ISO/IEC 27002

11.2.1. Kontroll 8.20 – annab tehnilised ja protseduurilised suunised võrgujuurdepääsu, segmenteerimise ja seire kaitsmiseks.

### 11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – nõuab infovoogude kontrolli võrkudes ja süsteemide vahel.

11.3.2. SC-7 – nõuab piirikaitset, turvalist marsruutimist ja võrgu segmenteerimist loata juurdepääsu riski vähendamiseks.

### 11.4. ELi GDPR

11.4.1. Artikkel 32 – nõuab asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada isikuandmeid töötlevate võrgustatud süsteemide ja teenuste konfidentsiaalsus, terviklus ja käideldavus.

### 11.5. ELi NIS2 direktiiv

11.5.1. Artikkel 21(2)(d) – nõuab riskipõhiseid tehnilisi meetmeid, sealhulgas võrguturvet ja juurdepääsukontrolli.

11.5.2. Artikkel 21(2)(e) – nõuab süsteemide segmenteerimist ja isoleerimist, et vältida küberintsidentide levikut.

### 11.6. ELi DORA

11.6.1. Artikkel 9 – nõuab, et ettevõtted rakendaksid IKT-riskijuhtimise kontrollimeetmeid, sealhulgas turvaliste võrkude ja side kaitseks.

11.6.2. Artikkel 10 – nõuab, et digitaalse toimepidevuse strateegia hõlmaks võrgutaristu ja kaugühenduvuse kaitset.

### 11.7. COBIT 2019

11.7.1. DSS05.02 – nõuab IT-taristu ja võrgukeskkondade tõhusat kaitset sisemiste ja väliste ohtude eest.

11.7.2. APO13.01 – nõuab riskijuhtimise strateegiaid, mis hõlmavad võrgu segmenteerimist ja seiret ohtude maandamise osana.