					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P21					Dokumendi pealkiri: **Võrguturbe 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 8	Ei kohaldu
ISO/IEC 27002:2022	Kontrollimeetmed 8.20-8.22	Ei kohaldu
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	Ei kohaldu
EL GDPR	Artikkel 32	Ei kohaldu
EL NIS2	Artikkel 21(2)(d)	Ei kohaldu
EL DORA	Artikkel 9	Ei kohaldu
COBIT 2019	DSS01.03, DSS05.01, MEA03	Ei kohaldu

1. Eesmärk

1.1 Käesoleva poliitika eesmärk on kehtestada organisatsiooni nõuded sise- ja välisvõrkude kaitsmiseks loata juurdepääsu, teenusehäirete, andmete pealtkuulamise ja väärkasutuse eest.

1.2 Sellega tagatakse, et kogu võrgutaristu, sealhulgas füüsiline, virtuaalne, pilvepõhine ja hübriidne taristu, on kaitstud kihiliste turvameetmetega, nagu võrgu segmenteerimine, tulemüürireeglite rakendamine, turvaline marsruutimine ja tsentraliseeritud seire.

1.3 Käesolev poliitika rakendab standardi ISO/IEC 27001 punkti 8.1 ja lisa A kontrollimeetmeid 8.20 kuni 8.22 ning tagab vastavuse kohaldatavatele õigus- ja regulatiivsetele nõuetele GDPR-i artikli 32, NIS2 artikli 21 ja DORA artikli 9 alusel.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõikidele võrkudele ja nendega seotud taristukomponentidele, sealhulgas:

2.1.1 marsruuterid, kommutaatorid, traadita pääsupunktid ja tulemüürid;

2.1.2 pilve virtuaalvõrgud (nt AWS VPC, Azure VNET), VPN-kontsentraatorid ja SD-WAN-süsteemid;

2.1.3 sisemised LAN-id, DMZ-d, kaugjuurdepääsuteed ning asukohtadevahelised või kolmandate osapoolte ühendused;

2.1.4 tugisüsteemid, nagu DNS, DHCP, puhverserverid ja seadmetel põhinevad seirelahendused.

2.2 Poliitika on siduv kogu personalile ja kolmandatest osapooltest teenuseosutajatele, kes haldavad, konfigureerivad, seiravad või kasutavad organisatsiooni võrkudega liidestuvaid lahendusi, sõltumata sellest, kas tegevus toimub kohapealses keskkonnas või pilvekeskkonnas.

2.3 Kõik organisatsiooni võrkudega ühendatud süsteemid ja rakendused, sõltumata nende asukohast või omandivormist, peavad vastama käesolevatele võrguturbe nõuetele.

3. Eesmärgid

3.1 Tagada üle võrkude edastatavate andmete konfidentsiaalsus, terviklus ja käideldavus tugeva juurdepääsukontrolli, turvalise marsruutimise ja seire kaudu.

3.2 Tõkestada loata juurdepääs, lateraalne liikumine ja võrguga ühendatud ressursside väärkasutamine, rakendades võrgu segmenteerimist, tsoonide eristamist ja perimeetrikaitset.

3.3 Hoida võrgu konfiguratsioonid järjepidevad, lähtudes valdkonna standarditest ja ohuteabest, et kaitsta arenevate küberohtude eest.

3.4 Kaitsta välissidet, pilveühenduvust ja kaugjuurdepääsu krüpteeritud kanalite, tugeva autentimise ja lõppseadmete valideerimise abil.

3.5 Tagada nähtavus võrgutegevuse üle tsentraliseeritud logimise, liikluse reaalajase kontrolli ja automaatsete teavituste kaudu.

3.6 Tagada õigusnormidele vastavus, viies kõik võrguoperatsioonid kooskõlla standardi ISO/IEC 27001:2022, GDPR-i, NIS2, DORA ja COBIT 2019 nõuetega.

4. Rollid ja vastutused

4.1 infoturbejuht (CISO)

4.1.1 Vastutab käesoleva poliitika eest ning tagab selle regulaarse läbivaatamise ja kooskõla organisatsiooni küberturbe strateegiaga.

4.1.2 Kiidab heaks võrgu segmenteerimise mudelid, tundlike süsteemide tulemüürireeglistikud ja eranditaotlused.

4.2 võrguturbe juht / taristuturbe juht

4.2.1 Haldab võrgu turbearhitektuuri, sealhulgas tulemüüre, sissetungi tuvastamise ja tõkestamise süsteeme (IDS/IPS), VPN-e ning turvalist marsruutimist.

4.2.2 Teostab järelevalvet võrgu segmenteerimise, VLAN-ide määratluste, liiklustsoonide ja välisühenduvuse üle.

4.2.3 Tagab sisse- ja väljamineva liikluse filtreerimise ning nullusalduse põhimõtete rakendamise pideva ülevaatamise kõigis võrgukihtides.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Võrguturbe juht peab koostöös CISO-ga käesoleva poliitika igal aastal läbi vaatama ja ajakohastama, lähtudes järgmistest asjaoludest:

9.1.1 uued ohud (nt uued ründetehnikad ja protokollide haavatavused);

9.1.2 taristu muudatused (nt pilvemigratsioonid ja SD-WAN-i juurutused);

9.1.3 võrgu kaitset mõjutavad regulatiivsed või standardimuudatused;

9.1.4 auditileiud, intsidentide trendid või kontrollimeetmetest tingitud toimivuse halvenemine.

9.2 Läbivaatamine tuleb algatada ka järgmistel juhtudel:

9.2.1 olulised muudatused võrguarhitektuuris;

9.2.2 uute tulemüüri-, VPN-i või pilvevõrgu platvormide kasutuselevõtt;

9.2.3 võtmevarade või usaldatud tsoonide kasutuselt kõrvaldamine.

9.3 Ajakohastused tuleb logida ISMS-i dokumendihalduse registris ja edastada järgmistele osapooltele:

9.3.1 taristu- ja võrguoperatsioonid;

9.3.2 SOC ja turbeinseneeria meeskonnad;

9.3.3 rakendusmeeskonnad, mille süsteemid sõltuvad võrguliiklusest;

9.3.4 kõik kolmandatest osapooltest tarnijad, kellel on aktiivne ühenduvus.

9.4 Kõik varasemad poliitika versioonid tuleb arhiveerida turvaliselt koos muudatuste ajaloo märkustega, et säilitada auditikõlblikkus ja muudatuste jälgitavus.

10. Seotud poliitikad ja seosed

10.1 P1 - Infoturbepoliitika. Sätestab infoturbe aluspõhimõtted ja nõuab kihiliste kaitsemeetmete rakendamist, sealhulgas võrgupõhist juurdepääsukontrolli ja ohtude vastaseid kontrollimeetmeid.

10.2 P4 - Juurdepääsukontrolli poliitika. Tagab, et võrgu segmenteerimist rakendatakse kooskõlas kasutajarollide, vähimate õiguste põhimõtte ja juurdepääsuõiguste andmise reeglitega.

10.3 P5 - Muudatuste haldamise poliitika. Reguleerib tulemüüri muudatusi, VPN-reeglite kohandamist ja marsruutimise muudatusi dokumenteeritud ning auditeeritava protsessi kaudu.

10.4 P12 - Varahalduse poliitika. Toetab võrku ühendatud süsteemide tuvastamist ja klassifitseerimist ning tagab, et kõiki ühendatud varasid hallatakse poliitikas määratletud kohaldamisala alusel.

10.5 P22 - Logimise ja seire poliitika. Reguleerib võrgulogide, sealhulgas tulemüüri sündmuste, juurdepääsukatsete ja anomaaliatuvastuste kogumist, korreleerimist ja säilitamist.

10.6 P30 - Intsidendihalduse poliitika. Määratleb eskaleerimise, ohjeldamise ja likvideerimise protseduurid vastuseks võrgupõhistele ohtudele või sissetungidele, nagu DDoS, lateraalne liikumine või loata juurdepääs.

11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on kooskõlas rahvusvaheliste standardite ja regulatiivsete nõuetega, mis määratlevad turvalised võrguoperatsioonid, võrgu segmenteerimise, perimeetrikaitse ja turvalise kaugjuurdepääsu.

11.2 ISO/IEC 27001

11.2.1 Punkt 8.1 - operatiivne planeerimine ja kontroll: nõuab tehniliste kontrollimeetmete, sealhulgas võrgukaitsemeetmete, lõimimist operatiivsetesse protsessidesse.

11.3 ISO/IEC 27002:2022

11.3.1 Kontrollimeetmed 8.20-8.22. Annab suunised võrkude kaitsmiseks, teenuste segmenteerimiseks ja võrguteenuste kaitsmiseks juurdepääsukontrolli ja seire abil.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - piirikaitse: nõuab perimeetrikontrolle, võrgu segmenteerimist ja turvalisi ühendusi.

11.4.2 AC-4 - teabevoogude jõustamine: toetab tsoonipõhist eristamist ja reeglipõhiseid liikluspiiranguid.

11.4.3 SC-32 - infosüsteemide eraldamine: edendab infosüsteemide loogilist eraldamist.

11.5 EL GDPR (2016/679)

11.5.1 Artikkel 32 - töötlemise turvalisus: nõuab tehnilisi meetmeid, näiteks tulemüüre ja võrgu segmenteerimist, isikuandmete kaitsmiseks.

11.6 EL NIS2 direktiiv (2022/2555)

11.6.1 Artikkel 21(2)(d): nõuab võrgu- ja infosüsteemide tõhusat turvet, perimeetrikaitset, turvalist konfiguratsiooni ning eraldusmeetmeid.

11.7 EL DORA (2022/2554)

11.7.1 Artikkel 9 - IKT-riskide juhtimine: kohustab finantssektori üksusi kaitsma võrke ja ühendusi loata juurdepääsu, andmelekkete ja tegevushäirete eest.

11.8 COBIT 2019

11.8.1 DSS01.03 - taristu seire: nõuab ennetavat kontrolli võrgu seisundi ja ühenduvuse üle.

11.8.2 DSS05.01 - kaitse pahavara vastu: hõlmab võrgu segmenteerimist ja perimeetrikaitset leviku minimeerimiseks.

11.8.3 MEA03 - vastavuse seire, hindamine ja auditeerimine: tugevdab võrgupoliitika rakendamist ja vastavushindamisi.