					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P35					Dokumendi pealkiri: **IoT/OT turbepoliitika**						
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 kohaldatavate standardite ja õigusnormidega

Kooskõla kohaldatavate standardite ja õigusnormidega

Standard/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	
ISO/IEC 27002:2022	Kontrollimeetmed 5.7, 5.23, 5.27, 5.31, 5.36	
NIST SP 800-53 Rev.5	SC-7, SI-4, CM-2, AC-6, PL-8	
EL isikuandmete kaitse üldmäärus (GDPR)	Artiklid 5, 25, 32	
EL NIS2 direktiiv	Artiklid 21, 23	
EL DORA	Artiklid 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Eesmärk

1.1 Käesolev poliitika kehtestab kohustuslikud infoturbenõuded asjade interneti (IoT) ja operatsioonitehnoloogia (OT) süsteemide juurutamiseks, käitamiseks, seireks ja kasutuselt kõrvaldamiseks organisatsioonis.

1.2 Sellega tagatakse, et nimetatud süsteemid on lõimitud organisatsiooni laiema küberturbe juhtimissüsteemiga ning kaitstud kompromiteerimise, väärkasutuse ja tööprotsesside saboteerimise eest.

1.3 Poliitika eesmärk on kehtestada tugevad tehnilised, organisatsioonilised ja menetluslikud kontrollimeetmed, et kaitsta IoT/OT süsteeme, mis on ühendatud füüsilise taristu, tootmisprotsesside ja ohutuskriitiliste keskkondadega.

1.4 Poliitika toetab küberturbe, ohutuse, keskkonnakontrolli ja toimepidevuse valdkondades kehtivaid regulatiivseid ning lepingulisi kohustusi.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigi IoT- ja OT-süsteemide suhtes, mida kasutatakse organisatsiooni töö-, haldus- või tootmiskeskkondades, sõltumata sellest, kas need kuuluvad ettevõttele, on renditud või kolmanda osapoole pakutud.

2.2 Hõlmatud süsteemid on muu hulgas järgmised:

2.2.1 IoT-seadmed, nagu keskkonnaandurid, läbipääsukontrollilahendused, nutivalgustus, valvevarustus ja kantavad seadmed

2.2.2 OT-platvormid, nagu PLC-d, SCADA, DCS, HMI-paneelid, MES-liidesed ja täiturseadmed

2.2.3 Tööstuslikud juhtimisvõrgud või pilvega ühendatud varad, mis seiravad füüsilisi tööprotsesse

2.3 Poliitika hõlmab:

2.3.1 Kõiki keskkondi (kohapealne, servataristu, pilvepõhiselt hallatav)

2.3.2 Kõiki osapooli (sisekasutajad, integraatorid, kolmandatest osapooltest tarnijad, töövõtjad)

2.3.3 Kõiki olelusringi etappe (projekteerimine, hankimine, juurutamine, käitamine, kasutuselt kõrvaldamine)

3. Eesmärgid

3.1 Kaitsta IoT- ja OT-taristut sisemiste ja väliste küberturbeohtude eest, sealhulgas teenusetõkestusrünnete, loata juurdepääsu, lunavararünde leviku ja püsivara muutmise eest.

3.2 Tagada, et IoT/OT-platvormid ei kujuneks IT- ja OT-keskkondade vaheliste rünnete vektoriks ega kompromiteeriks ohutuskriitilisi süsteeme.

3.3 Rakendada nende tehnoloogiate kogu olelusringi vältel turvalisus kavandamisel ja mitmekihilise kaitse põhimõtteid.

3.4 Võimaldada IoT- ja OT-platvormide usaldusväärne, turvaline ja auditivalmis lõimimine organisatsiooni turbeoperatsioonide keskuse (SOC) ning intsidentidele reageerimise plaanidega.

3.5 Tagada, et kõik juurutused vastavad ISO/IEC 27001 kontrollimeetmetele ja asjakohastele valdkondlikele juhistele (nt IEC 62443, ISO 27019, NIST SP 800-82).

4. Rollid ja vastutused

4.1 Infoturbejuht (CISO) / turbevaldkonna juht

4.1.1 Määratleb IoT/OT küberturbe poliitikad ja tehnilised standardid

4.1.2 Teeb järelevalvet riskihindamiste, kontrollimeetmete valideerimise ja osakondadevahelise koordineerimise üle

4.2 OT-insenerid / hoonete ja tootmisüksuste juhid

4.2.1 Valideerivad OT-süsteemide seadistused ja tagavad poliitika järgimise tootmisaladel

4.2.2 Hoiavad OT-süsteemide tervikluse ja ohutuse tagamiseks kehtivana füüsilised ning loogilised kaitsemeetmed

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

9.1 Käesolev poliitika tuleb läbi vaadata vähemalt kord aastas ja ajakohastada järgmiste asjaolude alusel:

9.1.1 Muudatused OT- või IoT-süsteemide arhitektuuris, tarnijates või platvormides

9.1.2 Olulised regulatiivsed uuendused (nt DORA, NIS2 või valdkondlike direktiivide muudatused)

9.1.3 Uute nõrkuste või ohumustrite ilmnemine juhtimissüsteemides

9.1.4 Sise- või välisauditite, penetratsioonitestide või red team'i harjutuste tulemused

9.2 Läbivaatamisprotsessi ühise algatamise eest vastutavad infoturbejuht (CISO), OT-turbejuht ja asjaomaste üksuste juhid.

9.3 Vaheülevaatus tuleb algatada pärast järgmist:

9.3.1 Iga IoT/OT-ga seotud intsident, mis põhjustab süsteemitõrke või andmekao

9.3.2 Olulise uue seadme, seiretarkvara või püsivaraplatvormi kasutuselevõtt

9.3.3 Nutika servaarvutuse või tehisintellektiga täiustatud automatiseerimise lõimimine välitasandil

9.4 Kõik poliitika muudatused tuleb:

9.4.1 Dokumenteerida versiooniajaloos ja poliitikamuudatuste registris

9.4.2 Teavitada kõigile mõjutatud kasutajatele, tarnijatele ja IT-/OT-operaatoritele

9.4.3 Kinnitada uuesti kõrgema juhtkonna poolt

10. Seotud poliitikad ja seosed

10.1 Käesolevat poliitikat rakendatakse koos järgmiste infoturbe poliitikatega ja nende toel:

10.1.1 P1 – Infoturbe poliitika: sätestab aluspõhimõtted, mis laienevad ka IoT- ja OT-süsteemide turbele.

10.1.2 P3 – Lubatava kasutuse poliitika: määratleb piirangud isiklike ja loata seadmete kasutamisele, sealhulgas töökeskkondades.

10.1.3 P6 – Riskijuhtimise poliitika: suunab manussüsteemide ja juhtimissüsteemidega seotud riskide hindamist, aktsepteerimist ja leevendamist.

10.1.4 P12 – Varahalduse poliitika: tagab, et kõik IoT- ja OT-süsteemid on ametlikult inventeeritud ja neile on määratud vastutavad omanikud.

10.1.5 P20 – Lõppseadmete kaitse / pahavara poliitika: kohaldub tootmiskeskkonnas ühendatud kontrolleritele, nutikatele lüüsidele ja servasüsteemidele.

10.1.6 P22 – Logimise ja seire poliitika: laieneb OT-keskkondade logikogumise ja läbivaatamise menetlustele.

10.1.7 P30 – Intsidentidele reageerimise poliitika: reguleerib otseselt, kuidas IoT/OT rikkumisi, anomaaliaid või süsteemitõrkeid tuleb eskaleerida ja hallata.

10.1.8 P33 – Auditi ja vastavusseire poliitika: sätestab kindlusmeetmed käesoleva poliitika pideva vastavuse valideerimiseks.

11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on kooskõlas rahvusvaheliselt tunnustatud standardite ja regulatiivsete raamistikega, mis tagavad asjade interneti (IoT) ja operatsioonitehnoloogia (OT) süsteemide turvalisuse, toimepidevuse ja vastavuse tööstus-, tootmis- ja ettevõttekeskkondades.

11.2 ISO/IEC 27002:2022 – Kontrollimeetmed 5.7, 5.23, 5.27, 5.31, 5.36

11.2.1 Kontrollimeede 5.7 – Ohuanalüüs ja ohuteave: toetab OT-keskkondade seiret ja IoT-spetsiifiliste nõrkuste tuvastamist.

11.2.2 Kontrollimeede 5.23 – Infoturve pilveteenuste kasutamisel: kohaldub juhul, kui IoT-seadmed liidestuvad pilveplatvormidega telemeetria, juhtimise või analüütika eesmärgil.

11.2.3 Kontrollimeede 5.27 – Turvaline süsteemiarhitektuur ja inseneripõhimõtted: reguleerib turvalisus kavandamisel põhimõtete rakendamist manussüsteemides ja juhtimisvõrkudes.

11.2.4 Kontrollimeede 5.31 – Turvalisus arendus- ja tugiprotsessides: nõuab tarkvara ja püsivara valideerimist, paikade kontrolli ning tarnijanõudeid OT-juurutustes.

11.2.5 Kontrollimeede 5.36 – Vastavus õiguslikele ja lepingulistele nõuetele: tagab OT-varade vastavuse ohutus-, keskkonna- ja regulatiivsetele nõuetele.

11.2.6 Need kontrollimeetmed moodustavad ühiselt parimad tavad IoT/OT-süsteemide kaitsmiseks kogu nende olelusringi jooksul, hõlmates arhitektuuri kavandamist, turvalist juurutamist, paikamist, anomaaliate tuvastamist ja valdkondlike nõuete täitmist.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Piirikaitse: tagab, et OT-võrgud on segmenteeritud ja kaitstud loata juurdepääsu eest.

11.3.2 SI-4 – Süsteemiseire: nõuab ICS-keskkondades pidevseire ja anomaaliatuvastuse mehhanismide rakendamist.

11.3.3 CM-2 – Lähteseadistus: nõuab IoT/OT-platvormide seadistuste kontrolli ja tugevdamist.

11.3.4 AC-6 – Vähimad õigused: kohaldub kasutajate juurdepääsule ja manustatud juhtimissüsteemide kaugteenindusele tarnijate poolt.

11.3.5 PL-8 – Turbe- ja privaatsusarhitektuurid: reguleerib turvalise süsteemilõimimise planeerimist, eriti OT ajakohastamise projektides.

11.4 EL isikuandmete kaitse üldmäärus (GDPR) (2016/679)

11.4.1 Artikkel 5 – Isikuandmete töötlemise põhimõtted: kohaldub IoT-platvormidele, mis töötlevad isikutega seotud anduri- või käitumuslikke andmeid.

11.4.2 Artikkel 25 – Andmekaitse kavandamisel ja vaikimisi: nõuab, et privaatsuskaitsemeetmed oleksid IoT-toodete disaini ja püsivarasse sisse ehitatud.

11.4.3 Artikkel 32 – Töötlemise turvalisus: nõuab nutiseadmete andmeedastuses krüptimist, juurdepääsukontrolli ja turvalist sidet.

11.5 EL NIS2 direktiiv (2022/2555)

11.5.1 Artiklid 21 ja 23: kehtestavad turbenõuded elutähtsatele ja olulistele üksustele, kes kasutavad OT-süsteeme. Need hõlmavad riskihindamist, intsidentidest teavitamist ning IoT/OT tarnijate ja püsivara tervikluse kontrolli tarneahelas.

11.6 EL DORA (2022/2554)

11.6.1 Artikkel 9 – IKT riskijuhtimine: nõuab manussüsteemide ja OT-tehnoloogiate turvalist lõimimist IKT riskijuhtimise programmi.

11.6.2 Artikkel 10 – IKT turbenõuded: nõuab kaitsemeetmeid omavahel ühendatud OT-platvormidele, mida kasutatakse finants- ja kriitiliste teenuste keskkondades.

11.7 COBIT 2019

11.7.1 DSS05.01 – Kaitse pahavara vastu: hõlmab ICS-spetsiifiliste ohtude ja IoT pahavarakampaaniate tuvastamist ning neile reageerimist.

11.7.2 BAI09.01 – Turbenõuete kehtestamine ja haldamine: seostub nutika või manustatud taristu turvalise kasutuselevõtu ja käitamisega.

11.7.3 APO13.02 – Infoturbeplaani kehtestamine ja haldamine: nõuab OT-süsteemide ja nende nõrkuste kaasamist organisatsiooniülesesse küberturbe strateegiasse.