					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P35S					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 standardite ja õigusaktidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrollid 5.23, 5.31	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
EL isikuandmete kaitse üldmäärus (GDPR)	Artikkel 32	
EL NIS2	Artikkel 21(2)(a), (d), (f)	
EL DORA	Artikkel 9(2), 10(1)	

1. Eesmärk

1.1. Käesolev poliitika sätestab kohustuslikud nõuded asjade interneti (IoT) ja operatsioonitehnoloogia (OT) seadmete turvaliseks kasutamiseks ja haldamiseks organisatsioonis. Nende seadmete hulka võivad kuuluda nutiandurid, turvakaamerad, tootmisseadmed, HVAC-kontrollerid või muud võrku ühendatud tööstussüsteemid.

1.2. Käesoleva poliitika eesmärk on:

1.2.1. kaitsta füüsilisi ja digitaalseid tegevusi häirete või manipuleerimise eest, mis võivad tuleneda ebapiisavalt kaitstud ühendatud seadmetest;

1.2.2. kehtestada IoT- ja OT-süsteemide turvalise juurutamise, seire ja hoolduse nõuded;

1.2.3. tagada vastavus standardile ISO/IEC 27001:2022, NIS2 direktiivile ja seotud regulatiivsetele raamistikele;

1.2.4. kehtestada VKE-dele praktilised ja rakendatavad kontrollimeetmed kontori-, lao- või tootmiskeskkonnas.

2. Kohaldamisala

2.1. Käesolev poliitika kehtib kõigile isikutele, kes osalevad IoT- või OT-seadmete planeerimises, paigaldamises, konfigureerimises, kasutamises, toetuses või kasutuselt kõrvaldamises. See hõlmab:

2.1.1. töötajaid, töövõtjaid või praktikante, kellel on seadmetele füüsiline või kaugjuurdepääs;

2.1.2. kolmandatest osapooltest tarnijaid või hooldustehnikuid, kes paigaldavad või hooldavad ühendatud süsteeme;

2.1.3. tegevjuhti või töötajaid, kes vastutavad turbepoliitikate järelevalve eest.

2.2. Poliitika hõlmab:

2.2.1. IoT-seadmeid, nagu nutlukud, valve- ja seiresüsteemid, nutiarvestid või printerid;

2.2.2. OT-süsteeme, sealhulgas PLC-sid (programmeeritavad loogikakontrollerid), SCADA-paneele või tööstuslüüse;

2.2.3. neid süsteeme toetavat riistvara, haldusrakendusi ja sidevõrke.

2.3. Käesolev poliitika kehtib kõikides töökohtades, sealhulgas kontorikeskkondades, kaugasukohtades, tootmisaladel ja pilveplatvormidel, mis on nende seadmetega liidestatud.

3. Eesmärgid

3.1. Turvaline juurutamine: tagada, et kõik IoT-/OT-süsteemid on enne töökeskkonnas kasutuselevõttu turvaliselt konfigureeritud.

3.2. Kokkupuute piiramine: vältida ühendatud seadmetele loata juurdepääsu, nende väärkasutust või ülevõtmist, rakendades tugevat juurdepääsukontrolli ja võrgu segmentimist.

3.3. Pidev seire: tagada nähtavus IoT-/OT-süsteemide toimimise üle tegevuste logimise ja ebahariliku käitumise seire kaudu.

3.4. Tarnijate vastutus: tagada, et kolmandatest osapooltest teenuseosutajad järgivad turvalise paigalduse, konfigureerimise ja hoolduse praktikaid.

3.5. Õigusnormidele vastavus: tõendada täielikku kooskõla kohaldatavate standarditega, nagu ISO 27001, GDPR (kui kogutakse isikuandmeid) ja NIS2, et tagada kriitilise taristu toimepidevus.

4. Rollid ja vastutus

4.1. Tegevjuht

4.1.1. vastutab üldiselt IoT- ja OT-süsteemide turbe eest;

4.1.2. kiidab käesoleva poliitika heaks ja tagab selle rakendamise kõigis tegevusvaldkondades;

4.1.3. kontrollib, et tarnijad ja töövõtjad järgivad turvalise seadistamise ja hoolduse praktikaid;

4.1.4. annab loa võrgujuurdepääsuks igale IoT-/OT-süsteemile.

4.2. Määratud töötaja või tegevusjuht (kui määratud)

4.2.1. teostab järelevalvet IoT-/OT-seadmete registri, paigutuse ja konfiguratsiooni üle;

4.2.2. registreerib iga seadme asukoha, võrgumääratluse ja toetava dokumentatsiooni;

4.2.3. tagab, et kõik muudatused (nt püsivara uuendused või seadmete asendused) on dokumenteeritud.

[... 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. Tegevjuht peab käesoleva poliitika läbi vaatama vähemalt üks kord aastas.

9.1.2. Läbivaatamisel tuleb hinnata, kas poliitika on jätkuvalt tõhus, hõlmab kehtivaid seadmetüüpe ning on kooskõlas uute riskide ja tehnoloogiatega.

9.2. Sündmuspõhised ajakohastused

9.2.1. Poliitika ajakohastamine tuleb algatada ka juhul, kui:

9.2.2. võetakse kasutusele uut tüüpi IoT- või OT-süsteemid;

9.2.3. tarnijad väljastavad turvateateid või teateid elutsükli lõppemise kohta;

9.2.4. intsident või audit tuvastab puudujääke IoT-/OT-kontrollimeetmetes;

9.2.5. uued õigusaktid või standardid kehtestavad täiendavaid nõudeid.

9.3. Dokumentatsioon ja versioonihaldus

9.3.1. Kõik ajakohastused tuleb dokumenteerida, sealhulgas kuupäev, versiooninumber ja muudatuste kokkuvõte.

9.3.2. Tegevjuht peab säilitama poliitika varasemad versioonid auditi eesmärgil.

9.4. Muudatustest teavitamine

9.4.1. Kõik poliitika muudatused tuleb edastada kõigile asjaomastele töötajatele ja tarnijatele.

9.4.2. Uuendatud versioonid peavad olema kättesaadavad ühiskaustades või paigalduskohtades või juhtimiskeskustes paberkandjal.

10. Seotud poliitikad ja seosed

10.1. Käesolevat poliitikat tuleb rakendada kooskõlas järgmiste seotud VKE poliitikatega:

10.1.1. P4S – juurdepääsukontrolli poliitika: kehtestab seadmetaseme sisselogimiskontrollid, tugevate paroolide kasutamise ja volitatud juurdepääsu protseduurid IoT- ja OT-platvormidele;

10.1.2. P9S – kaugtöö poliitika: välistab kaugjuurdepääsu kasutamise IoT-/OT-juhtpaneelidele ebaturvaliste või heakskiitmata kanalite kaudu;

10.1.3. P17S – andmekaitse ja privaatsuse poliitika: kohaldub juhul, kui IoT-seadmed (nt turvakaamerad) töötlevad või salvestavad isikuandmeid, tagades vastavuse GDPR-ile;

10.1.4. P30S – intsidentidele reageerimise poliitika: sätestab protseduurid IoT- või OT-intsidentide tuvastamiseks, neist teatamiseks ja nende lahendamiseks, sealhulgas rikkumise kahtluse või talitlushäire korral;

10.1.5. P36S – sotsiaalmeedia ja väliskommunikatsiooni poliitika: tagab, et seadmete kohta käivat teavet ega võrgu ülesehitust ei jagata väljapoole ilma heakskiiduta.

10.2. Iga seotud poliitika tugevdab käesoleva poliitika rakendamist ja praktilist kasutamist, pakkudes sihipäraseid protseduurilisi juhiseid.

11. Viitestandardid ja raamistikud

11.1. ISO/IEC 27001

11.1.1. Punkt 6.1 – riskide tuvastamine ja käsitlemine: nõuab, et IoT- ja OT-süsteemidega seotud riske hinnatakse ja maandatakse süstemaatiliselt.

11.1.2. Punkt 8.1 – tegevuste planeerimine ja ohje: tagab ühendatud seadmete turvalise operatiivse ohje.

11.2. ISO/IEC 27002

11.2.1. Kontroll 5.23 – operatsioonitehnoloogia kasutamise infoturve: määratleb OT turvalise kasutamise füüsilistes ja digitaalsetes keskkondades.

11.2.2. Kontroll 5.31 – infosüsteemide turvaline konfiguratsioon: nõuab IoT-/OT-seadmetele kõvendatud seadistusi ja ebaturvaliste vaikeseadete vältimist.

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – tarkvara, püsivara ja teabe terviklus: nõuab püsivara ja uuenduste tervikluse valideerimist.

11.3.2. CM-7 – minimaalne funktsionaalsus: seadmetel ei tohi olla lubatud kasutamata või ebaturvalisi funktsioone.

11.3.3. AC-6 – vähimate õiguste põhimõte: juurdepääs seadmetele peab olema piiratud ainult volitatud kasutajatele.

11.3.4. PE-20 – varade seire: IoT- ja OT-varade füüsiline ja operatiivne seire.

11.3.5. SC-7 – piirikaitse: ühendatud süsteemide võrgusuhtluse segmentimine ja kontroll.

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

11.4.1. Artikkel 32 – töötlemise turvalisus: kui kogutakse isikuandmeid (näiteks valvekaamerate kaudu), peab organisatsioon rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid sellise töötlemise kaitsmiseks.

11.5. EL NIS2 direktiiv (2022/2555)

11.5.1. Artikkel 21(2)(a) – riskijuhtimismeetmed.

11.5.2. Artikkel 21(2)(d) – seadmete turvaline konfiguratsioon ja kasutamine.

11.5.3. Artikkel 21(2)(f) – tarneahela ja süsteemide turve.

11.6. EL DORA (2022/2554)

11.6.1. Artikkel 9(2) – IKT-riski juhtimise kohaldamisala: hõlmab töökeskkondades kasutatavaid tööstuslikke ja manussüsteemseid seadmeid.

11.6.2. Artikkel 10(1) – IKT toimepidevus: nõuab, et seadmete konfiguratsioonid toetaksid vastupidavust ja taastetoiminguid.

11.7. COBIT 2019

11.7.1. DSS01 – tegevuste juhtimine: kohaldub tehnoloogiliste tegevuste, sealhulgas füüsiliste seadmete järelevalvele.

11.7.2. DSS05 – turbeteenuste juhtimine: tagab, et ühendatud süsteeme jälgitakse ja kaitstakse nõuetekohaselt.

11.7.3. APO13 – turbe juhtimine: tugevdab poliitikaid, mis kaitsevad VKE-des kasutatavaid operatiivseid varasid.