					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P35					Dokumenta nosaukums: **IoT / OT drošības politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņojums ar standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	
ISO/IEC 27002:2022	Kontroles pasākumi 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	
GDPR	5., 25., 32. pants	
NIS2	21., 23. pants	
DORA	9., 10. pants	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Mērķis

1.1 Šī politika nosaka obligātās informācijas drošības prasības lietu interneta (IoT) un operatīvo tehnoloģiju (OT) sistēmu ieviešanai, ekspluatācijai, uzraudzībai un ekspluatācijas pārtraukšanai organizācijā.

1.2 Tā nodrošina, ka šīs sistēmas ir integrētas organizācijas kopējā kiberdrošības pārvaldības sistēmā un aizsargātas pret kompromitēšanu, neatbilstošu izmantošanu vai darbības sabotāžu.

1.3 Politikas mērķis ir noteikt stingrus tehniskos, organizatoriskos un procesuālos kontroles pasākumus, lai aizsargātu IoT/OT sistēmas, kas mijiedarbojas ar fizisko infrastruktūru, ražošanas procesiem un drošībkritiskām vidēm.

1.4 Tā atbalsta normatīvo un līgumisko pienākumu izpildi kiberdrošības, drošuma, vides kontroles un darbības nepārtrauktības jomā.

2. Tvērums

2.1 Šī politika attiecas uz visām IoT un OT sistēmām neatkarīgi no tā, vai tās pieder organizācijai, ir nomātas vai nodrošinātas no trešajām pusēm, un kuras tiek izmantotas organizācijas operacionālajā, administratīvajā vai ražošanas vidē.

2.2 Tvērumā ietilpst, bet neaprobežojas ar:

2.2.1 IoT ierīcēm, piemēram, vides sensoriem, piekļuves kontroles risinājumiem, viedā apgaismojuma iekārtām, novērošanas aprīkojumam un valkājamām ierīcēm

2.2.2 OT platformām, piemēram, PLC, SCADA, DCS, HMI paneļiem, MES saskarnēm un lauka kontrolieriem

2.2.3 Industriālajiem vadības tīkliem vai ar mākoņpakalpojumiem savienotiem aktīviem, kas uzrauga fiziskās darbības

2.3 Politika attiecas uz:

2.3.1 Visām vidēm (lokālajām, malas skaitļošanas un mākoņpārvaldītām)

2.3.2 Visām iesaistītajām pusēm (iekšējiem lietotājiem, integratoriem, trešo pušu piegādātājiem un darbuzņēmējiem)

2.3.3 Visām dzīvescikla fāzēm (projektēšanu, iepirkumu, ieviešanu, ekspluatāciju un ekspluatācijas pārtraukšanu)

3. Mērķi

3.1 Aizsargāt IoT un OT infrastruktūru pret iekšējiem un ārējiem kiberdrošības apdraudējumiem, tostarp pakalpojumatteices uzbrukumiem, neatļautu piekļuvi, izspiedējprogrammatūras izplatīšanos un manipulācijām ar aparātprogrammatūru.

3.2 Nodrošināt, ka IoT/OT platformas nekļūst par vektoru IT–OT tilta uzbrukumiem vai drošībkritisku sistēmu kompromitēšanai.

3.3 Piemērot drošības pēc projektēšanas un daudzslāņu aizsardzības principus visā šo tehnoloģiju dzīvesciklā.

3.4 Nodrošināt uzticamu, drošu un auditējamu IoT un OT platformu integrāciju organizācijas drošības operāciju centrā (SOC) un incidentu reaģēšanas plānos.

3.5 Nodrošināt, ka visas ieviešanas atbilst ISO/IEC 27001 kontroles pasākumiem un piemērojamajām nozares vadlīnijām (piemēram, IEC 62443, ISO 27019, NIST SP 800-82).

4. Lomas un pienākumi

4.1 Informācijas drošības vadītājs (CISO) / drošības vadītājs

4.1.1 Nosaka IoT/OT kiberdrošības politikas un tehniskos standartus

4.1.2 Pārrauga riska izvērtēšanu, kontroles pasākumu validāciju un starpstruktūrvienību koordināciju

4.2 OT inženieri / objektu un ražotņu vadītāji

4.2.1 Validē OT sistēmu konfigurācijas un nodrošina politikas prasību ievērošanu ražošanas zonās

4.2.2 Uztur fiziskos un loģiskos aizsardzības pasākumus OT integritātei un drošumam

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika jāpārskata vismaz reizi gadā un jāatjaunina, pamatojoties uz:

9.1.1 Izmaiņām OT vai IoT sistēmu arhitektūrā, piegādātājos vai platformās

9.1.2 Būtiskiem normatīvā regulējuma atjauninājumiem (piemēram, DORA, NIS2 vai nozaru direktīvu grozījumiem)

9.1.3 Jaunu ievainojamību vai apdraudējumu modeļu parādīšanos vadības sistēmās

9.1.4 Iekšējo vai ārējo auditu, penetrācijas testu vai sarkanās komandas vingrinājumu konstatējumiem

9.2 CISO, OT drošības vadītājs un attiecīgo struktūrvienību vadītāji ir kopīgi atbildīgi par pārskatīšanas procesa uzsākšanu.

9.3 Starpposma pārskatīšana jāierosina pēc:

9.3.1 Jebkura ar IoT/OT saistīta incidenta, kura rezultātā radusies sistēmas atteice vai datu zudums

9.3.2 Būtisku jaunu iekārtu, uzraudzības programmatūras vai aparātprogrammatūras platformu ieviešanas

9.3.3 Viedās malas skaitļošanas vai ar MI papildinātas automatizācijas integrācijas lauka līmenī

9.4 Visām politikas izmaiņām jābūt:

9.4.1 Dokumentētām versiju vēsturē un politikas izmaiņu reģistrā

9.4.2 Paziņotām visiem ietekmētajiem lietotājiem, piegādātājiem un IT/OT operatoriem

9.4.3 Atkārtoti apstiprinātām izpildvadības līmenī

10. Saistītās politikas un sasaistes

10.1 Šī politika darbojas kopā ar turpmāk minētajām informācijas drošības politikām un ir ar tām savstarpēji saistīta:

10.1.1 P1 – Informācijas drošības politika: nosaka drošības pamatprincipus, kas attiecas arī uz IoT un OT sistēmu drošību.

10.1.2 P3 – Pieļaujamās lietošanas politika: nosaka ierobežojumus personisko un neautorizētu ierīču lietošanai, tostarp operacionālajās vidēs.

10.1.3 P6 – Riska pārvaldības politika: nosaka kārtību riska izvērtēšanai, akceptēšanai un mazināšanai attiecībā uz iegultajām un vadības sistēmām.

10.1.4 P12 – Aktīvu pārvaldības politika: nodrošina, ka visas IoT un OT sistēmas ir formāli iekļautas uzskaitē un tām ir noteikti atbildīgie īpašnieki.

10.1.5 P20 – Galiekārtu aizsardzības / ļaunatūras politika: attiecas uz savienotiem kontrolieriem, viedajām vārtejām un malas sistēmām ražošanā.

10.1.6 P22 – Žurnalēšanas un uzraudzības politika: attiecas arī uz žurnālu iegūšanas un pārskatīšanas procedūrām OT vidēs.

10.1.7 P30 – Incidentu reaģēšanas politika: tieši nosaka, kā IoT/OT pārkāpumi, anomālijas vai sistēmu atteices jāeskalē un jāpārvalda.

10.1.8 P33 – Audita un atbilstības uzraudzības politika: nodrošina pārliecības mehānismus nepārtrauktas atbilstības šai politikai validēšanai.

11. Atsauces standarti un ietvari

11.1 Šī politika ir saskaņota ar starptautiski atzītiem standartiem un regulatīvajiem ietvariem, kas nodrošina lietu interneta (IoT) un operatīvo tehnoloģiju (OT) sistēmu drošību, noturību un atbilstību industriālajās, ražošanas un organizāciju vidēs.

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

11.2.1 Kontroles pasākums 5.7 – Apdraudējumu izlūkošana: nosaka OT vides uzraudzību un IoT specifisku ievainojamību identificēšanu.

11.2.2 Kontroles pasākums 5.23 – Informācijas drošība mākoņpakalpojumu izmantošanā: attiecas uz gadījumiem, kad IoT ierīces saskaras ar mākoņplatformām telemetrijas, vadības vai analītikas nolūkos.

11.2.3 Kontroles pasākums 5.27 – Droša sistēmu arhitektūra un inženierijas principi: nosaka drošības pēc projektēšanas principus iegultajām sistēmām un vadības tīkliem.

11.2.4 Kontroles pasākums 5.31 – Drošība izstrādes un atbalsta procesos: nosaka programmatūras un aparātprogrammatūras validāciju, ielāpu kontroles pasākumus un piegādātāju prasības OT ieviešanā.

11.2.5 Kontroles pasākums 5.36 – Atbilstība juridiskajām un līgumiskajām prasībām: nodrošina OT aktīvu atbilstību drošuma, vides un regulatīvajām prasībām.

11.2.6 Šie kontroles pasākumi kopumā nosaka labo praksi IoT/OT sistēmu aizsardzībai visā to dzīvesciklā, tostarp arhitektūras projektēšanā, drošā ieviešanā, ielāpošanā, anomāliju noteikšanā un atbilstībā nozares prasībām.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Robežu aizsardzība: nodrošina, ka OT tīkli ir segmentēti un aizsargāti pret neatļautu piekļuvi.

11.3.2 SI-4 – Sistēmu uzraudzība: nosaka nepārtrauktas uzraudzības un anomāliju noteikšanas mehānismu ieviešanu ICS vidēs.

11.3.3 CM-2 – Bāzlīnijas konfigurācija: nosaka konfigurācijas kontroli un IoT/OT platformu drošu konfigurēšanu.

11.3.4 AC-6 – Minimālās piekļuves tiesības: attiecas uz lietotāju piekļuvi un attālinātu piegādātāju apkalpošanu iegultajām vadības sistēmām.

11.3.5 PL-8 – Drošības un privātuma arhitektūras: nosaka drošas sistēmu integrācijas plānošanu, īpaši OT modernizācijas projektos.

11.4 GDPR (2016/679)

11.4.1 5. pants – Principi attiecībā uz personas datu apstrādi: attiecas uz IoT platformām, kas apstrādā ar sensoriem iegūtus vai uzvedības datus, kuri saistīti ar fiziskām personām.

11.4.2 25. pants – Datu aizsardzība pēc projektēšanas un pēc noklusējuma: nosaka, ka privātuma aizsardzības pasākumi jāiestrādā IoT produktu projektēšanā un aparātprogrammatūrā.

11.4.3 32. pants – Apstrādes drošība: nosaka šifrēšanu, piekļuves kontroli un drošus sakarus viedo ierīču datu pārraidei.

11.5 NIS2 direktīva (2022/2555)

11.5.1 21. un 23. pants: nosaka drošības pienākumus būtiskām un svarīgām vienībām, kas izmanto OT sistēmas. Tie ietver riska izvērtēšanu, ziņošanu par incidentiem un IoT/OT piegādātāju un aparātprogrammatūras integritātes pārbaudi piegādes ķēdē.

11.6 DORA (2022/2554)

11.6.1 9. pants – IKT riska pārvaldība: nosaka iegulto sistēmu un OT tehnoloģiju drošu integrāciju IKT riska pārvaldības programmā.

11.6.2 10. pants – IKT drošības prasības: nosaka aizsardzības pasākumus savstarpēji savienotām OT platformām, ko izmanto finanšu un kritisko pakalpojumu vidēs.

11.7 COBIT 2019

11.7.1 DSS05.01 – Aizsardzība pret ļaunatūru: ietver ICS specifisku apdraudējumu un IoT ļaunatūras kampaņu noteikšanu un reaģēšanu.

11.7.2 BAI09.01 – Drošības prasību noteikšana un uzturēšana: attiecas uz viedās vai iegultās infrastruktūras drošu nodrošināšanu un ekspluatāciju.

11.7.3 APO13.02 – Informācijas drošības plāna noteikšana un uzturēšana: nosaka, ka organizācijas mēroga kiberdrošības stratēģijā jāiekļauj OT sistēmas un to ievainojamības.