| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Šeit ievadiet reģistrētās juridiskās personas nosaukumu | | | | | | | |
| Dokumenta numurs:<br>P35S | | | | | Dokumenta nosaukums:<br>**IoT / OT drošības politika** | | | | | | | |
| Versija:<br>1.0 | | Spēkā stāšanās datums:<br>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** |
| | | | |
| | | | |

Saskaņots ar piemērojamiem standartiem un normatīvajiem aktiem

| Standarts/regulējums | Punkts/pants | Piezīme |
|---|---|---|
| ISO/IEC 27001:2022 | Punkti 6.1, 6.2, 8 | |
| ISO/IEC 27002:2022 | Kontroles pasākumi 5.23, 5 | |
| NIST SP 800-53 Rev.5 | SI-7, CM-7, AC-6, PE-20, SC-7 | |
| ES VDAR | 32. pants | |
| ES NIS2 | 21. panta 2. punkta a), d), f) apakšpunkts | |
| ES DORA | 9. panta 2. punkts, 10. panta 1. punkts | |

**1. Mērķis**

1.1. Šī politika nosaka obligātās prasības lietu interneta (IoT) un operacionālo tehnoloģiju (OT) ierīču drošai izmantošanai un pārvaldībai organizācijā. Šādas ierīces var ietvert viedos sensorus, drošības kameras, ražošanas iekārtas, HVAC kontrolierus vai jebkuras tīklam pieslēgtas rūpnieciskās sistēmas.

**1.2. Šīs politikas mērķis ir:**

1.2.1. aizsargāt fiziskās un digitālās darbības no traucējumiem vai manipulācijām, ko rada nepietiekami aizsargātas pieslēgtās ierīces;

1.2.2. nodrošināt drošu IoT un OT sistēmu ieviešanu, uzraudzību un uzturēšanu;

1.2.3. nodrošināt atbilstību ISO/IEC 27001:2022, NIS2 direktīvai un saistītajiem normatīvajiem ietvariem;

1.2.4. noteikt praktiskus un izpildāmus kontroles pasākumus MVU, kas darbojas biroju, noliktavu vai ražošanas vidēs.

**2. Piemērošanas joma**

**2.1. Šī politika attiecas uz visām personām, kas ir iesaistītas IoT vai OT ierīču plānošanā, uzstādīšanā, konfigurēšanā, izmantošanā, atbalstā vai norakstīšanā. Tas ietver:**

2.1.1. darbiniekus, līgumdarbiniekus vai praktikantus ar fizisku vai attālinātu piekļuvi ierīcēm;

2.1.2. trešo pušu piegādātājus vai servisa tehniķus, kas uzstāda vai uztur pieslēgtās sistēmas;

2.1.3. ģenerāldirektoru vai personālu, kas atbild par drošības politiku uzraudzību.

**2.2. Politika aptver:**

2.2.1. IoT ierīces, piemēram, viedās slēdzenes, videonovērošanas sistēmas, viedos skaitītājus vai printerus;

2.2.2. OT sistēmas, tostarp programmējamos loģiskos kontrolierus (PLC), SCADA paneļus vai rūpnieciskās vārtejas;

2.2.3. atbalsta aparatūru, pārvaldības lietotnes un sakaru tīklus, ko izmanto šīs sistēmas.

2.3. Šī politika ir piemērojama visās darba vietās: biroju vidēs, attālinātās vietās, ražošanas zonās un mākoņplatformās, kas saskaras ar šīm ierīcēm.

**3. Mērķi**

3.1. Droša ieviešana: jānodrošina, ka visas IoT/OT sistēmas pirms to ieviešanas ražošanas vidē ir droši konfigurētas.

3.2. Pakļautības ierobežošana: jānovērš neautorizēta piekļuve, nepareiza lietošana vai pieslēgto ierīču pārņemšana, piemērojot stingru piekļuves kontroli un tīkla segmentēšanu.

3.3. Nepārtraukta uzraudzība: jānodrošina pārredzamība pār IoT/OT darbību, veicot žurnalēšanu un uzraugot neparastu uzvedību.

3.4. Piegādātāju pārskatatbildība: jānodrošina, ka trešo pušu pakalpojumu sniedzēji ievēro drošas uzstādīšanas, konfigurēšanas un uzturēšanas prakses.

3.5. Normatīvā atbilstība: jāspēj pierādīt pilnīgu atbilstību piemērojamajiem standartiem, piemēram, ISO 27001, VDAR (ja tiek vākti personas dati) un NIS2 prasībām kritiskās infrastruktūras noturības jomā.

**4. Lomas un pienākumi**

**4.1. Ģenerāldirektors (GM)**

4.1.1. ir vispārēji atbildīgs par IoT un OT sistēmu drošību;

4.1.2. apstiprina šo politiku un nodrošina tās ieviešanu visās darbības zonās;

4.1.3. pārliecinās, ka piegādātāji un līgumdarbinieki ievēro drošas uzstādīšanas un uzturēšanas prakses;

4.1.4. autorizē tīkla piekļuvi jebkurai IoT/OT sistēmai.

**4.2. Norīkotais darbinieks vai operāciju vadītājs (ja ir norīkots)**

4.2.1. pārrauga IoT/OT ierīču uzskaiti, izvietošanu un konfigurēšanu;

4.2.2. reģistrē katras ierīces atrašanās vietu, tīkla piešķīrumu un pavaddokumentāciju;

4.2.3. nodrošina, ka jebkuras izmaiņas (piemēram, aparātprogrammatūras atjauninājumi vai ierīču nomaiņa) tiek dokumentētas.

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

**9. Pārskatīšanas un atjaunināšanas prasības**

**9.1. Ikgadējā pārskatīšana**

9.1.1. Šī politika GM jāpārskata vismaz reizi gadā.

9.1.2. Pārskatīšanā jāizvērtē, vai politika joprojām ir efektīva, aptver aktuālos ierīču tipus un atbilst jauniem riskiem vai tehnoloģijām.

**9.2. Atjaunināšana ierosinošu notikumu gadījumā**

9.2.1. Politikas atjauninājumi jāveic arī tad, ja:

9.2.2. tiek ieviesti jauni IoT vai OT sistēmu tipi;

9.2.3. piegādātāji izdod drošības paziņojumus vai paziņojumus par dzīves cikla beigām;

9.2.4. incidents vai audits identificē trūkumus IoT/OT kontroles pasākumos;

9.2.5. jauni normatīvie akti vai standarti nosaka papildu prasības.

**9.3. Dokumentācija un versiju kontrole**

9.3.1. Visi atjauninājumi jādokumentē, norādot datumu, versijas numuru un izmaiņu kopsavilkumu.

9.3.2. GM saglabā politikas vēsturiskās versijas audita vajadzībām.

**9.4. Izmaiņu paziņošana**

9.4.1. Par jebkādiem politikas atjauninājumiem jāinformē viss attiecīgais personāls un piegādātāji.

9.4.2. Atjauninātajām versijām jābūt pieejamām koplietojamās mapēs vai drukātā veidā uzstādīšanas vietās vai vadības centros.

**10. Saistītās politikas un sasaiste**

**10.1. Šī politika jāievieš saskaņā ar šādām saistītajām MVU politikām:**

10.1.1. P4S – Piekļuves kontroles politika: nosaka ierīču līmeņa pieteikšanās kontroles pasākumus, drošu paroļu izmantošanu un autorizētas piekļuves procedūras IoT un OT platformām;

10.1.2. P9S – Attālinātā darba politika: nepieļauj attālinātās piekļuves izmantošanu IoT/OT paneļiem pa nedrošiem vai neapstiprinātiem kanāliem;

10.1.3. P17S – Datu aizsardzības un privātuma politika: piemērojama, ja IoT ierīces (piemēram, drošības kameras) apstrādā vai ieraksta personas datus, nodrošinot atbilstību VDAR;

10.1.4. P30S – Incidentu reaģēšanas politika: nosaka procedūras IoT vai OT incidentu atklāšanai, ziņošanai un novēršanai, tostarp aizdomu par manipulācijām vai darbības atteici gadījumos;

10.1.5. P36S – Sociālo mediju un ārējās komunikācijas politika: nodrošina, ka informācija par ierīcēm vai tīkla izkārtojumu netiek izpausta ārpus organizācijas bez apstiprinājuma.

10.2. Katra saistītā politika stiprina šīs politikas ievērošanu un praktisko piemērošanu, sniedzot mērķētu procesuālu vadību.

## 11. Atsauces standarti un ietvari

### 11.1. ISO/IEC 27001

11.1.1. 6.1. punkts – risku identificēšana un apstrāde: nosaka, ka ar IoT un OT sistēmām saistītie riski sistemātiski jāizvērtē un jāmazina.

11.1.2. 8.1. punkts – darbības plānošana un kontrole: nodrošina drošus darbības kontroles pasākumus pieslēgtajām ierīcēm.

### 11.2. ISO/IEC 27002

11.2.1. 5.23. kontrole – informācijas drošība operacionālo tehnoloģiju (OT) sistēmu izmantošanā: nosaka drošu OT izmantošanu fiziskajās un digitālajās vidēs.

11.2.2. 5.31. kontrole – droša informācijas sistēmu konfigurēšana: nosaka prasību izmantot droši konfigurētas IoT/OT ierīces un izvairīties no nedrošiem noklusējuma iestatījumiem.

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

11.3.1. SI-7 – programmatūras, aparātprogrammatūras un informācijas integritāte: nosaka aparātprogrammatūras un atjauninājumu integritātes validēšanu.

11.3.2. CM-7 – minimālās funkcionalitātes princips: ierīcēs nedrīkst būt iespējotas neizmantotas vai nedrošas funkcijas.

11.3.3. AC-6 – minimālo privilēģiju princips: piekļuve ierīcēm jāierobežo tikai autorizētiem lietotājiem.

11.3.4. PE-20 – aktīvu uzraudzība: IoT un OT aktīvu fiziskā un operacionālā uzraudzība.

11.3.5. SC-7 – robežu aizsardzība: tīkla komunikācijas segmentēšana un kontrole pieslēgtajām sistēmām.

### 11.4. ES VDAR (2016/679)

11.4.1. 32. pants – apstrādes drošība: ja tiek iegūti personas dati (piemēram, ar novērošanas kamerām), organizācijai jāievieš atbilstoši tehniskie un organizatoriskie pasākumi šādas apstrādes aizsardzībai.

### 11.5. ES NIS2 direktīva (2022/2555)

11.5.1. 21. panta 2. punkta a) apakšpunkts – riska pārvaldības pasākumi.

11.5.2. 21. panta 2. punkta d) apakšpunkts – droša ierīču konfigurēšana un izmantošana.

11.5.3. 21. panta 2. punkta f) apakšpunkts – piegādes ķēdes un sistēmu drošība.

### 11.6. ES DORA (2022/2554)

11.6.1. 9. panta 2. punkts – IKT risku pārvaldības tvērums: ietver rūpnieciskās un iegultās ierīces, kas tiek izmantotas operacionālajās vidēs.

11.6.2. 10. panta 1. punkts – IKT nepārtrauktība: nosaka, ka ierīču konfigurācijām jāatbalsta noturība un atjaunošanas darbības.

**11.7. COBIT 2019**

11.7.1. DSS01 – darbību pārvaldība: attiecas uz tehnoloģisko darbību pārraudzību, tostarp fiziskajām ierīcēm.

11.7.2. DSS05 – drošības pakalpojumu pārvaldība: nodrošina, ka pieslēgtās sistēmas tiek pienācīgi uzraudzītas un aizsargātas.

11.7.3. APO13 – drošības pārvaldība: stiprina politikas operacionālo aktīvu aizsardzībai MVU vidē.