| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Šeit ievadiet reģistrētās juridiskās personas nosaukumu | | | | | | | |
| Dokumenta numurs:<br>P26S | | | | | Dokumenta nosaukums:<br>**Trešo pušu un piegādātāju 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** |
| | | | |
| | | | |

Saskaņotība ar standartiem un regulējumu

| Standarts/regulējums | Punkts/pants | Piezīme |
|---|---|---|
| ISO/IEC 27001:2022 | 8. punkts | Operatīvās kontroles prasības trešo pušu un piegādātāju attiecībām |
| ISO/IEC 27002:2022 | Kontroles pasākumi 5.19–5.22 | Piegādātāju drošības kontroles pasākumi, līgumiskie drošības nosacījumi, izmaiņu pārvaldība, uzraudzība un pārskatīšana |
| NIST SP 800-53 Rev.5 | SA-9, SA-10, CA-3, PS-7 | Iepirkuma, konfigurācijas, starpsavienojumu vienošanos un ārējā personāla kontroles pasākumi |
| ES GDPR | 28., 32. pants | Datu apstrādes līgumi, apstrādātāju drošības prasības |
| ES NIS2 | 21. panta 2. punkta a), b), i) apakšpunkts; 23. panta 1. punkts | Piegādes ķēdes risku pārvaldība, trešo pušu pakalpojumu uzraudzība |
| ES DORA | 5. panta 1., 2. punkts; 28. panta 1., 2. punkts | IKT risku pārvaldība attiecībā uz trešo pušu pakalpojumu sniedzējiem |
| COBIT 2019 | APO10, APO12, DSS05 | Piegādātāju pārvaldība un risku integrēšana |

**1. Mērķis**

1.1 Šī politika nosaka obligātās drošības prasības attiecību ar trešajām pusēm un piegādātājiem uzsākšanai, pārvaldībai un izbeigšanai, ja tie piekļūst organizācijas datiem, sistēmām vai pakalpojumiem vai tos ietekmē.

1.2 Tā nodrošina, ka ārējie pakalpojumu sniedzēji, tostarp IT atbalsta piegādātāji, mākoņpakalpojumu sniedzēji, programmatūras izstrādātāji un biznesa procesu ārpakalpojumu sniedzēji, uzņēmuma aktīvus apstrādā droši un atbilstoši piemērojamajiem tiesību aktiem un standartiem.

1.3 Šī politika mazina tādus riskus kā datu noplūde, neatļautas izmaiņas sistēmās, regulatīvās sankcijas vai darbības traucējumi, ko izraisa nedroši vai nepietiekami pārvaldīti sadarbības modeļi ar trešajām pusēm.

**2. Piemērošanas joma**

**2.1 Šī politika attiecas uz visām trešajām pusēm, kas:**

2.1.1 nodrošina programmatūru, infrastruktūru, mitināšanas vai mākoņpakalpojumus;

2.1.2 piekļūst iekšējām sistēmām, ierīcēm vai lietotnēm vai tās pārvalda;

2.1.3 apstrādā uzņēmuma datus, dokumentus vai rezerves kopijas;

2.1.4 atbalsta uzņēmuma darbību, personāla vadību, finanšu funkcijas vai klientu apkalpošanu.

**2.2 Tā attiecas arī uz:**

2.2.1 iekšējiem darbiniekiem, kas iesaistīti piegādātāju atlasē, piesaistē vai uzraudzībā;

2.2.2 personālu, kas pārvalda piegādātāju sākotnējo izvērtēšanu, līgumus, piekļuves tiesības vai pārskatīšanu;

2.2.3 jebkuru sistēmu vai procesu, kas ir atkarīgs no trešo pušu komponentēm vai pakalpojumiem.

**3. Mērķi**

3.1 Nodrošināt, ka visi piegādātāji atbilst skaidri noteiktām drošības prasībām.

3.2 Noteikt, ka piegādātāju līgumos obligāti jāiekļauj izpildāmas drošības, privātuma un incidentu pārvaldības saistības.

3.3 Pirms līgumu noslēgšanas vai piekļuves piešķiršanas izvērtēt un dokumentēt piegādātāju riskus.

3.4 Augsta riska vai darbībkritisku piegādātāju gadījumā veikt regulāru pārskatīšanu, lai apstiprinātu atbilstību.

3.5 Noteikt formālu kārtību izņēmumu pārvaldībai, incidentu pārvaldībai un līgumu atjaunināšanai.

3.6 Atbalstīt atbilstību ISO/IEC 27001:2022, GDPR, NIS2 un DORA prasībām attiecībā uz piegādātāju pārvaldību.

**4. Lomas un atbildība**

**4.1 Vispārējais vadītājs (GM)**

4.1.1 Uzņemas galīgo atbildību par piegādātāju atlasi un drošības atbilstību.

4.1.2 Apstiprina ar piegādātājiem saistītos līgumus, izņēmumus un eskalācijas gadījumus.

4.1.3 Uzrauga incidentu pārvaldību un lēmumu pieņemšanu gadījumos, kad piegādātāji nepilda savas saistības.

**4.2 IT pakalpojumu sniedzējs vai iekšējā drošības kontaktpersona**

4.2.1 Izvērtē piegādātāju pieprasīto tehnisko piekļuvi.

4.2.2 Ievieš piekļuves kontroles prasības, pārskata žurnālus un pārbauda drošu datu apstrādi.

4.2.3 Ja piemērojams, pārskata pierādījumus par drošības kontroles pasākumiem, sertifikāciju vai audita rezultātiem.

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

**9. Pārskatīšanas un atjaunināšanas prasības**

9.1 Šī politika Vispārējam vadītājam jāpārskata vismaz reizi gadā, iesaistot IT pakalpojumu sniedzēju vai piegādātāju pārvaldnieku.

**9.2 Politika jāpārskata arī:**

9.2.1 pēc jebkādām būtiskām izmaiņām tiesiskajos, regulatīvajos vai līgumiskajos pienākumos;

9.2.2 pēc ar piegādātāju saistīta drošības incidenta vai audita konstatējuma;

9.2.3 ieviešot jaunas piegādātāju kategorijas (piemēram, darbībkritiskas SaaS platformas).

**9.3 Visiem atjauninājumiem jābūt:**

9.3.1 dokumentētiem ar versiju vēsturi un pamatojumu;

9.3.2 apstiprinātiem no Vispārējā vadītāja puses;

9.3.3 paziņotiem attiecīgajiem iekšējiem darbiniekiem un piegādātāju pārvaldniekiem;

9.3.4 glabātiem kopā ar iepriekšējām versijām saskaņā ar politiku P14S – Datu glabāšanas un drošas iznīcināšanas politika.

**10. Saistītās politikas un sasaistes**

**10.1 Šīs politikas efektivitāte ir atkarīga no koordinācijas ar šādām MVU informācijas drošības politikām:**

10.1.1 P2S – Pārvaldības lomu un atbildības politika: nosaka atbildību par piegādātāju uzraudzību un līgumu prasību izpildi.

10.1.2 P4S – Piekļuves kontroles politika: nosaka piekļuves ierobežošanas prasības, kas jāpiemēro, piešķirot piegādātājiem piekļuvi sistēmām.

10.1.3 P17S – Datu aizsardzības un privātuma politika: nodrošina, ka piegādātāji, kuri apstrādā personas datus, ievēro datu aizsardzības principus un tiesiskās prasības.

10.1.4 P14S – Datu glabāšanas un drošas iznīcināšanas politika: attiecas uz jebkādiem datiem vai ierakstiem, kas kopīgoti ar piegādātājiem vai tiek glabāti pie tiem, un nosaka drošas iznīcināšanas kārtību pēc līguma izbeigšanas.

10.1.5 P30S – Incidentu pārvaldības politika: nosaka rīcību gadījumos, kad piegādātājs izraisa drošības incidentu vai ir tajā iesaistīts, tostarp eskalācijas un pierādījumu apstrādes kārtību.

10.2 Šīs politikas kopumā nodrošina, ka piegādātāju risks tiek kontrolēts visā līguma darbības ciklā.

## 11. Atsauces standarti un ietvari

### 11.1 ISO/IEC 27001

11.1.1 8. punkts nosaka operatīvo kontroles pasākumu ieviešanu, tostarp pasākumus, kas piemērojami trešo pušu un piegādātāju attiecībām.

### 11.2 ISO/IEC 27002

11.2.1 Kontroles pasākums 5.19 nodrošina, ka piegādātāju drošības pasākumi ir saskaņoti ar organizācijas prasībām.

11.2.2 Kontroles pasākums 5.20 nosaka formālas vienošanās, kas aptver drošības nosacījumus, atbildību un pienākumus pārkāpumu gadījumā.

11.2.3 Kontroles pasākums 5.21 regulē izmaiņas piegādātāju pakalpojumos, kas var ietekmēt drošības stāvokli.

11.2.4 Kontroles pasākums 5.22 nosaka piegādātāju pakalpojumu un atbilstības uzraudzību un pārskatīšanu.

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

11.3.1 SA-9 regulē ārējo sistēmu un pakalpojumu iegādi, pieprasot risku izvērtēšanu un skaidri noteiktas prasības.

11.3.2 SA-10 nosaka konfigurācijas un izmaiņu procedūru kontroli sistēmām, ko pārvalda trešās puses.

11.3.3 CA-3 nosaka starpsavienojumu vienošanos nepieciešamību sistēmām, kurās iesaistītas ārējas personas vai organizācijas.

11.3.4 PS-7 nosaka prasības ārējā personāla pārbaudei un atbildībai.

### 11.4 ES GDPR (2016/679)

11.4.1 28. pants nosaka datu apstrādes līgumu nepieciešamību ar piegādātājiem, kuri darbojas kā apstrādātāji.

11.4.2 32. pants nosaka atbilstošus tehniskos un organizatoriskos drošības pasākumus visiem datu apstrādātājiem.

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

11.5.1 21. panta 2. punkta a), b), i) apakšpunkts nosaka IKT piegādes ķēdes risku pārvaldību un trešo pušu kontroles pasākumus.

11.5.2 23. panta 1. punkts nosaka dokumentētu trešo pušu pakalpojumu uzraudzību būtiskajiem un svarīgajiem subjektiem.

### 11.6 ES DORA (2022/2554)

11.6.1 5. panta 1. punkts nosaka IKT risku pārvaldības satvaru, kas aptver visus kritiskos trešo pušu pakalpojumu sniedzējus.

11.6.2 5. panta 2. punkts nosaka līgumiskos un operatīvos kontroles pasākumus IKT pakalpojumu atkarībām.

11.6.3 28. panta 1. un 2. punkts nosaka uzraudzības prasības finanšu nozares IKT trešo pušu riskam.

**11.7 COBIT 2019**

11.7.1 APO10 – “Piegādātāju pārvaldība” nosaka prasības iepirkuma kontroles pasākumiem un attiecību pārvaldībai.

11.7.2 APO12 – “Risku pārvaldība” integrē piegādātāju risku organizācijas risku pārvaldībā.

11.7.3 DSS05 – “Drošības pakalpojumu pārvaldība” attiecas uz pārvaldītiem trešo pušu un ārpakalpojumu sniedzējiem.