| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Šeit ievadiet reģistrētās juridiskās personas nosaukumu | | | | | | | |
| Dokumenta numurs:<br>P27S | | | | | Dokumenta nosaukums:<br>**Mākoņpakalpojumu izmantošanas 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** |
| | | | |
| | | | |

Saskaņota ar piemērojamiem standartiem un regulējumu

| Standarts/regulējums | Punkts/pants | Piezīme |
|---|---|---|
| ISO/IEC 27001:2022 | 8. punkts | |
| ISO/IEC 27002:2022 | 5.23.–5.25. kontroles pasākumi | |
| NIST SP 800-53 Rev. 5 | AC-20, SC-12, SC-13, SR-5 | |
| ES Vispārīgā datu aizsardzības regula (VDAR) | 28. pants, 32. pants un V nodaļa | |
| ES NIS2 | 21. panta 2. punkta f) un i) apakšpunkts | |
| ES DORA | 5. panta 2. punkts, 28. pants | |
| COBIT 2019 | DSS01, DSS05, BAI04 | |

**1. Mērķis**

1.1 Šī politika nosaka prasības drošai mākoņpakalpojumu izmantošanai organizācijā. Tā nodrošina, ka mākoņvidē apstrādātie vai glabātie dati ir aizsargāti, piekļuve ir kontrolēta un riski tiek pārvaldīti atbildīgi.

1.2 Tā palīdz MVU izpildīt tiesiskos pienākumus un klientu prasības attiecībā uz sensitīvas informācijas aizsardzību, datu noplūžu novēršanu un ar mākoņpakalpojumiem saistīto risku efektīvu pārvaldību bez uzņēmuma mēroga infrastruktūras.

1.3 Šī politika atbalsta ISO/IEC 27001 sertifikāciju, atbilstību VDAR un piegādes ķēdes apliecinājumu, nodrošinot konsekventu visu trešo pušu mākoņpakalpojumu pārvaldību.

**2. Piemērošanas joma**

**2.1 Šī politika attiecas uz:**

2.1.1 jebkuru mākoņpakalpojumu, ko izmanto uzņēmuma datu glabāšanai, apstrādei vai pārsūtīšanai;

2.1.2 visu personālu, līgumslēdzējiem vai pakalpojumu sniedzējiem, kuri organizācijas vārdā izmanto mākoņrīkus;

2.1.3 bezmaksas un maksas mākoņrisinājumiem, tostarp e-pasta platformām, dokumentu koplietošanai, SaaS rīkiem, rezerves kopēšanas platformām, videokonferenču risinājumiem un klientu platformām;

2.1.4 jebkuru ierīci (galddatoru, mobilo ierīci, planšetdatoru), ar kuru caur mākoņlietotnēm piekļūst uzņēmuma informācijai.

**2.2 Tā ietver, bet neaprobežojas ar:**

2.2.1 Microsoft 365, Google Workspace, Dropbox Business;

2.2.2 Zoom, Microsoft Teams, Google Meet;

2.2.3 AWS, Azure, GCP;

2.2.4 mākoņpakalpojumu rezerves kopēšanas un avārijas atjaunošanas rīkiem;

2.2.5 koplietotām mapēm vai lietotnēm, ko izmanto rēķinu izrakstīšanai, projektu vadībai vai saziņai ar klientiem.

**3. Mērķi**

3.1 Novērst neatļautu vai augsta riska neapstiprinātu mākoņpakalpojumu izmantošanu.

3.2 Nodrošināt, ka mākoņvidē glabātie sensitīvie vai regulēti dati tiek aizsargāti ar atbilstošiem tehniskajiem un organizatoriskajiem kontroles pasākumiem.

3.3 Noteikt skaidras lomas mākoņpakalpojumu apstiprināšanai, konfigurēšanai, uzraudzībai un ekspluatācijas pārtraukšanai.

3.4 Kontrolēt datu plūsmas un nodrošināt glabāšanas, dzēšanas un privātuma prasību izpildi attiecībā uz mākoņvidē glabāto informāciju.

3.5 Samazināt paļaušanos uz personīgajiem kontiem vai neuzskaitītiem rīkiem, nodrošinot visu biznesa vajadzībām izmantoto mākoņsistēmu apstiprināšanu.

3.6 Ievērot ISO/IEC 27001:2022, VDAR, NIS2 un DORA prasības ārējo mākoņatkarību pārvaldībai.

**4. Lomas un pienākumi**

**4.1 Ģenerāldirektors (GM)**

4.1.1 apstiprina visu jauno mākoņpakalpojumu izmantošanu;

4.1.2 pārskata riskus, kas saistīti ar mākoņpakalpojumu sniedzējiem un pakalpojumu veidiem;

4.1.3 nodrošina politikas ievērošanu un pārrauga lēmumus par izņēmumiem.

**4.2 Ārējais IT pakalpojumu sniedzējs vai tehniskā atbalsta funkcija**

4.2.1 izvērtē un ievieš drošas konfigurācijas mākoņpakalpojumiem;

4.2.2 izveido kontus, piekļuves kontroles pasākumus un rezerves kopijas;

4.2.3 uzrauga atbilstību paroļu, daudzfaktoru autentifikācijas (MFA) un drošības iestatījumu prasībām.

[ ... 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 ģenerāldirektoram sadarbībā ar ārējo IT pakalpojumu sniedzēju.

**9.2 Formāla pārskatīšana jāveic arī:**

9.2.1 pēc ar mākoņpakalpojumiem saistīta drošības incidenta (piemēram, pārkāpuma, datu zuduma);

9.2.2 kad tiek ieviesta jauna būtiska mākoņplatforma;

9.2.3 ja mainās tiesiskās vai regulatīvās prasības (piemēram, VDAR, NIS2, DORA atjauninājumi);

9.2.4 ja uzraudzības darbības atklāj nepareizu lietošanu vai jaunus riskus.

**9.3 GM jānodrošina, ka:**

9.3.1 Mākoņpakalpojumu reģistrs tiek atjaunināts ar jauniem vai izņemtiem pakalpojumiem;

9.3.2 tiesiskās un privātuma prasības joprojām tiek izpildītas;

9.3.3 visas izmaiņas tiek paziņotas attiecīgajiem lietotājiem un iesaistītajām pusēm.

9.4 Arhivētās versijas jāuzglabā droši, un vecās politikas versijas jāapstrādā saskaņā ar organizācijas P14S – Datu uzglabāšanas politika un Datu likvidēšanas politiku.

**10. Saistītās politikas un sasaiste**

**10.1 Šī politika jāpiemēro kopā ar šādām MVU vajadzībām pielāgotām informācijas drošības politikām:**

10.1.1 P2S – Pārvaldības lomu un atbildības politika: nosaka pārskatatbildību par mākoņpakalpojumu apstiprināšanu un attiecību pārvaldību ar pakalpojumu sniedzējiem.

10.1.2 P4S – Piekļuves kontroles politika: atbalsta drošas pieteikšanās, sesiju pārvaldības un piekļuves tiesību atsaukšanas praksi, kas nepieciešama mākoņplatformām.

10.1.3 P14S – Datu uzglabāšanas politika un Datu likvidēšanas politika: nosaka, kā mākoņvidē glabātie dati tiek dublēti, glabāti un dzēsti atbilstoši tiesiskajiem pienākumiem.

10.1.4 P17S – Datu aizsardzības un privātuma politika: nodrošina, ka visi mākoņpakalpojumos glabātie personas dati tiek apstrādāti saskaņā ar VDAR principiem.

10.1.5 P30S – Incidentu reaģēšanas politika: nosaka strukturētas procedūras reaģēšanai uz mākoņdrošības incidentiem, tostarp pierādījumu materiālu vākšanai un ārējai paziņošanai.

10.2 Kopā šīs politikas nodrošina, ka mākoņpakalpojumu izmantošana ir droša, atbilstoša un darbības ziņā noturīga.

## 11. Atsauces standarti un ietvari

### 11.1 ISO/IEC 27001

11.1.1 8. punkts — nosaka, ka organizācijām jāievieš darbības kontroles pasākumi datu apstrādei, tostarp attiecībā uz mākoņvidē izvietotām sistēmām.

### 11.2 ISO/IEC 27002

11.2.1 5.23. kontrole — nosaka pārvaldības prasības mākoņpakalpojumu un trešo pušu SaaS rīku izmantošanai.

11.2.2 5.24. kontrole — paredz pienākumu noteikt mākoņpakalpojumu izmantošanas politiku, kas saskaņota ar riska un regulatīvajām prasībām.

11.2.3 5.25. kontrole — paredz pienākumu organizācijām nodrošināt, ka drošības kontroles pasākumi mākoņvidē atbilst organizācijas vajadzībām.

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

11.3.1 AC-20 — paredz formālas lietošanas politikas ārējām sistēmām, piemēram, mākoņpakalpojumiem.

11.3.2 SC-12, SC-13 — attiecas uz šifrēšanu datiem pārsūtē un glabāšanā mākoņvidē.

11.3.3 SR-5 — aptver mākoņpakalpojumu un trešo pušu riska kontroles pasākumus piegādes ķēdē.

### 11.4 ES Vispārīgā datu aizsardzības regula (2016/679)

11.4.1 28. pants — nosaka, ka mākoņpakalpojumu sniedzējiem, kuri darbojas kā apstrādātāji, jāievēro saistoši līgumiski pienākumi.

11.4.2 32. pants — nosaka tehniskos un organizatoriskos kontroles pasākumus mākoņvidē balstītai datu apstrādei.

11.4.3 V nodaļa — aizliedz neatļautu personas datu starptautisku pārsūtīšanu, ja tie glabājas mākoņvidē.

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

11.5.1 21. panta 2. punkta f) un i) apakšpunkts — nosaka, ka būtiskajām un svarīgajām vienībām jāievieš atbilstošas politikas mākoņpakalpojumu drošībai un piegādes ķēdes kontrolei.

### 11.6 ES DORA (2022/2554)

11.6.1 5. panta 2. punkts — nosaka, ka finanšu MVU mākoņdrošība jāintegrē savos IKT risku pārvaldības ietvaros.

11.6.2 28. pants — nosaka pārraudzības noteikumus kritiskiem trešo pušu IKT pakalpojumu sniedzējiem, tostarp mākoņpakalpojumu sniedzējiem.

### 11.7 COBIT 2019

11.7.1 DSS01 — “Pārvaldīt operācijas” attiecas uz mākoņpakalpojumu darbības integritāti.

11.7.2 DSS05 — “Pārvaldīt drošības pakalpojumus” ietver mākoņpakalpojumiem specifiskus aizsardzības un uzraudzības pasākumus.

11.7.3 BAI04 — “Pārvaldīt pieejamību un kapacitāti” nodrošina darbības nepārtrauktību un veiktspēju mākoņvidē.