					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P27					Dokumenta nosaukums: **Mākoņpakalpojumu izmantošanas 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**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	Prasības mākoņvides darbību plānošanai un kontrolei.
ISO/IEC 27002:2022	Kontroles pasākumi 5.23–5.25	Prasības attiecībā uz mākoņpakalpojumu izmantošanu, politiku un drošību.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12–SC-28, SR-5	Ārējo sistēmu izmantošana, līgumiskās un tehniskās prasības, kriptogrāfiskie aizsardzības pasākumi, piegādes ķēdes aizsardzība.
ES GDPR	28. pants, 32. pants, V nodaļa	Prasības mākoņpakalpojumu apstrādātājiem, apstrādes drošībai un datu pārsūtīšanai.
ES NIS2	21. panta 2. punkta f) un i) apakšpunkts	Trešo pušu riska un piegādes ķēdes prasības.
ES DORA	5. panta 2. punkts, 28. pants	IKT un trešo pušu mākoņpakalpojumu pārraudzība finanšu iestādēm.
COBIT 2019	BAI04, DSS01, DSS05	Mākoņpakalpojumu pieejamības, operāciju un drošības pārvaldība.

1. Mērķis

1.1 Šī politika nosaka organizācijas obligātās prasības drošai, atbilstošai un atbildīgai mākoņdatošanas pakalpojumu izmantošanai visos pakalpojumu sniegšanas modeļos: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) un Software-as-a-Service (SaaS).

1.2 Politikas mērķis ir nodrošināt, ka mākoņpakalpojumi tiek ieviesti un pārvaldīti tā, lai aizsargātu informācijas aktīvu konfidencialitāti, integritāti un pieejamību (CIA), vienlaikus izpildot regulatīvās, tiesiskās un līgumiskās prasības.

1.3 Tā nosaka kontroles pasākumus mākoņrisku pārvaldībai, datu aizsardzībai, pakalpojumu sniedzēju atbilstības uzraudzībai un nesankcionētas izmantošanas novēršanai. Tā arī atbalsta uzņēmējdarbības inovācijas, izmantojot mākoņplatformas, saskaņojot drošību, darbības uzticamību un izmaksu efektivitāti.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visiem darbiniekiem, līgumslēdzējiem, trešo personu pakalpojumu sniedzējiem un ārējiem konsultantiem, kuri organizācijas vārdā nodrošina, konfigurē, izmanto, pārvalda mākoņpakalpojumus vai piekļūst tiem.

2.2 Tā attiecas uz visām vidēm, kurās tiek apstrādāti organizācijas dati vai darbslodzes, tostarp:

2.2.1 publiskās, privātās, hibrīdās un koplietotās mākoņvides izvietošanas modeļiem;

2.2.2 visiem mākoņpakalpojumu modeļiem (IaaS, PaaS, SaaS);

2.2.3 vairāku mākoņu un federētām arhitektūrām;

2.2.4 Shadow IT vai personīgu mākoņkontu izmantošanai uzņēmējdarbības vajadzībām.

2.3 Tā aptver visus datu klasifikācijas līmeņus un attiecas gan uz iekšējām sistēmām, gan uz piegādātāju mitinātām platformām, kurās tiek glabāti vai apstrādāti organizācijai piederoši vai reglamentēti dati.

3. Mērķi

3.1 Nodrošināt drošu un konsekventu mākoņtehnoloģiju izmantošanu, izmantojot skaidri noteiktas lietošanas prasības, drošības bāzlīnijas un pārvaldības lomas.

3.2 Samazināt ar mākoņdatošanu saistītos darbības un regulatīvos riskus, tostarp nesankcionētu piekļuvi, datu aizsardzības pārkāpumus, nepareizu konfigurāciju, neatbilstību un pakalpojumu darbības traucējumus.

3.3 Nodrošināt drošības un privātuma prasību piemērošanu visiem mākoņpakalpojumu sniedzējiem un pārbaudīt atbilstību, izmantojot līguma klauzulas, izvērtēšanu un audita tiesības.

3.4 Veicināt mērogojamu un noturīgu mākoņpakalpojumu ieviešanu, nepasliktinot drošības stāvokli, tiesisko prasību izpildi vai darbības nepārtrauktību.

3.5 Saskaņot mākoņpakalpojumu pārvaldību un izmantošanu ar organizācijas IDPS ietvaru, tiesiskajiem pienākumiem (piemēram, GDPR, DORA), nozares vadlīnijām un nozarē atzītu labo praksi (piemēram, NIST, COBIT).

4. Lomas un pienākumi

4.1 Izpildvadība

4.1.1 Apstiprina Mākoņpakalpojumu izmantošanas politiku un stratēģisko mākoņpakalpojumu ieviešanas ceļvedi.

4.1.2 Pārskata un apstiprina augsta riska izņēmumus no standarta mākoņpakalpojumu pārvaldības prasībām.

4.1.3 Nodrošina, ka mākoņpakalpojumu iniciatīvām tiek piešķirts pietiekams finansējums, pārraudzība un integrācija uzņēmuma risku pārvaldības ietvarā.

4.2 Galvenais informācijas drošības vadītājs (CISO)

4.2.1 Ir šīs politikas un organizācijas Mākoņpakalpojumu reģistra īpašnieks.

4.2.2 Apstiprina jaunu mākoņpakalpojumu sniedzēju ieviešanu, pamatojoties uz pienācīgu rūpību un riska izvērtējumu.

4.2.3 Pārskata pakalpojumu sniedzēju atbilstības dokumentāciju un apstiprina atbilstību drošības 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 un pēc vajadzības jāatjaunina, lai nodrošinātu nepārtrauktu atbilstību:

9.1.1 mainīgajām tiesiskajām un regulatīvajām prasībām (piemēram, GDPR, NIS2, DORA);

9.1.2 izmaiņām ISO/IEC 27001 vai ISO/IEC 27002 standartos;

9.1.3 atjauninājumiem organizācijas mākoņarhitektūrā, risku vidē vai pakalpojumu portfelī;

9.1.4 incidentu izmeklēšanas rezultātiem, auditu rezultātiem vai ekspluatācijas atziņām.

9.2 CISO ir atbildīgs par pārskatīšanas uzsākšanu un attiecīgo iesaistīto pušu sasaukšanu, tostarp:

9.2.1 Mākoņdrošības arhitektu;

9.2.2 juridiskās un atbilstības funkcijas komandas;

9.2.3 iepirkumu un piegādātāju pārvaldības vadītājus;

9.2.4 pakalpojumu īpašniekus un IT operācijas.

9.3 Visiem atjauninājumiem jābūt:

9.3.1 pārvaldītiem versiju kontrolē un datētiem;

9.3.2 apstiprinātiem izpildvadībā;

9.3.3 paziņotiem skartajām pusēm, tostarp darbiniekiem, līgumslēdzējiem un trešajām pusēm;

9.3.4 arhivētiem saskaņā ar iekšējām dokumentu pārvaldības politikām.

9.4 Starpposma pārskatīšanu var ierosināt:

9.4.1 jaunas sadarbības uzsākšana ar CSP vai būtiskas migrācijas;

9.4.2 jauni apdraudējumi mākoņinfrastruktūrai;

9.4.3 būtiskas izmaiņas līgumiskajos, tiesiskajos vai nozarei specifiskajos pienākumos.

10. Saistītās politikas un sasaiste

10.1 Šī politika ir cieši saistīta ar šādām iekšējām politikām un ir no tām atkarīga:

10.1.1 P1 – Informācijas drošības politika: nosaka vispārīgos principus drošai sistēmu un pakalpojumu darbībai, kurus šī politika piemēro mākoņpakalpojumu kontekstā.

10.1.2 P5 – Izmaiņu pārvaldības politika: visām mākoņkonfigurācijas izmaiņām jāievēro P5 noteiktās izmaiņu kontroles procedūras.

10.1.3 P13 – Datu klasifikācijas un marķēšanas politika: nosaka, kā dati tiek izvērtēti pirms pārsūtīšanas uz mākoņvidi un kā tiek piemēroti tādi kontroles pasākumi kā šifrēšana un datu rezidence.

10.1.4 P18 – Kriptogrāfisko kontroles pasākumu politika: nosaka standartus šifrēšanai, atslēgu pārvaldībai un kriptogrāfisko algoritmu izmantošanai, kas ir tieši piemērojami mākoņpakalpojumu konfigurācijās.

10.1.5 P22 – Žurnālfiksēšanas un uzraudzības politika: nosaka prasības žurnālu vākšanai, glabāšanai un analīzei, kas jāpiemēro mākoņvidēs.

10.1.6 P30 – Incidentu reaģēšanas politika: nosaka eskalācijas, ierobežošanas un trūkumu novēršanas procedūras ar mākoņpakalpojumiem saistītiem drošības notikumiem.

10.1.7 P33 – Audita un atbilstības uzraudzības politika: atbalsta gatavību auditam un nepārtrauktu pārliecību, ka mākoņpakalpojumu kontroles pasākumi ir ieviesti un uzraudzīti.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001: 8.1. punkts – darbību plānošana un kontrole: nosaka, ka organizācijām jāievieš un jākontrolē procesi, kas nepieciešami informācijas drošības prasību izpildei, tostarp procesi, kas skar mākoņvides.

11.2 ISO/IEC 27002:2022 – kontroles pasākumi 5.23 līdz 5.25:

11.2.1 A pielikuma 5.23. kontrole – mākoņpakalpojumu izmantošana: nosaka uz risku balstītu izvērtēšanu, formālu autorizāciju un mākoņpakalpojumu izmantošanas dokumentēšanu.

11.2.2 A pielikuma 5.24. kontrole – mākoņpakalpojumu izmantošanas politika: nosaka prasību izveidot un piemērot formālu mākoņpakalpojumu izmantošanas politiku, kas atbilst organizācijas vajadzībām un riskiem.

11.2.3 A pielikuma 5.25. kontrole – drošība mākoņpakalpojumos: nosaka nepieciešamību nodrošināt drošības integrāciju, līgumiskos aizsardzības pasākumus un mākoņvidē izvietotu darbslodžu un datu uzraudzību.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – ārējo sistēmu izmantošana: nosaka definētus noteikumus un nosacījumus piekļuvei organizācijas resursiem no ārējām vai mākoņpakalpojumos balstītām sistēmām.

11.3.2 SA-9(5) – ārējo informācijas sistēmu pakalpojumi: nosaka līgumiskās drošības prasības, pārraudzību un nepārtrauktu uzraudzību trešo pušu mākoņsistēmām.

11.3.3 SC-12 līdz SC-28 – kriptogrāfiskie aizsardzības pasākumi, perimetra aizsardzība un pārsūtīšanas integritāte: atbilst šifrēšanas, identitāšu un piekļuves prasībām mākoņvidē izvietotiem pakalpojumiem un datiem pārsūtē.

11.3.4 SR-5 – piegādes ķēdes aizsardzība: atbalsta CSP pārbaudi un līgumisko kontroli pakalpojumu sniegšanas procesā.

11.4 ES GDPR (2016/679):

11.4.1 28. pants – apstrādātāja pienākumi: nosaka prasību slēgt formālus līgumus ar mākoņpakalpojumu sniedzējiem, lai nodrošinātu personas datu apstrādes drošību, konfidencialitāti un auditējamību.

11.4.2 32. pants – apstrādes drošība: atbalsta šifrēšanas, piekļuves kontroles, žurnālfiksēšanas un citu drošības pasākumu piemērošanu mākoņvidēs.

11.4.3 V nodaļa – starptautiska datu pārsūtīšana: nosaka likumīgu datu pārsūtīšanu ārpus ES/EEZ, izmantojot aizsardzības pasākumus, piemēram, SCC vai atbilstības lēmumus.

11.5 ES NIS2 direktīva (2022/2555):

11.5.1 21. panta 2. punkta f) un i) apakšpunkts: nosaka pienākumu organizācijām pārvaldīt riskus, ko rada trešo pušu mākoņpakalpojumu sniedzēji, un nodrošināt digitālās piegādes ķēdes integritāti, izmantojot līgumiskus un tehniskus pasākumus.

11.6 ES DORA (2022/2554):

11.6.1 5. panta 2. punkts – IKT risku pārvaldība: nosaka prasību integrēt IKT trešo pušu risku, tostarp mākoņpakalpojumu risku, kopējā risku pārvaldībā.

11.6.2 28. pants – kritisko IKT trešo pušu pakalpojumu sniedzēju pārraudzība: nosaka prasību finanšu iestādēm uzraudzīt, kontrolēt un sniegt pārskatus par atkarību no mākoņpakalpojumu sniedzējiem, to drošības stāvokli un noturību.

11.7 COBIT 2019:

11.7.1 BAI04 – pieejamības un kapacitātes pārvaldība: nodrošina, ka mākoņpakalpojumi ir noturīgi, uzraudzīti un atbilst noteiktiem veiktspējas kritērijiem.

11.7.2 DSS01 – operāciju pārvaldība: atbalsta darbību integrāciju, incidentu apstrādi un pamatkonfigurācijas mākoņvidē izvietotās platformās.

11.7.3 DSS05 – drošības pakalpojumu pārvaldība: nosaka mākoņpakalpojumiem specifisku drošības kontroles pasākumu ieviešanu, uzraudzību un incidentu novēršanu digitālajos pakalpojumos.