					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P27S					Dokumento pavadinimas: **Debesijos paslaugų naudojimo politika**							
Versija: 1.0		Įsigaliojimo data: 01.01.2025			Dokumento savininkas:							
X	Politika		Standartas		Procedūra		Forma		Registras		Kita	

Peržiūrų istorija				
Peržiūros numeris	**Peržiūros data**	**Pakeitimai**	**Peržiūrėjo**	**Proceso savininkas**

Patvirtinimai			
Vardas	**Pareigos**	**Data**	**Parašas**

Suderinta su standartais ir reglamentais

Standartas / reglamentas	Skyrius / straipsnis	Pastaba
ISO/IEC 27001:2022	8 skyrius	
ISO/IEC 27002:2022	Kontrolės priemonės 5.23–5.25	
NIST SP 800-53 Rev. 5	AC-20, SC-12, SC-13, SR-5	
ES BDAR	28, 32 straipsniai ir V skyrius	
ES NIS2 direktyva	21 straipsnio 2 dalies f ir i punktai	
ES DORA reglamentas	5 straipsnio 2 dalis, 28 straipsnis	
COBIT 2019	DSS01, DSS05, BAI	

1. Tikslas

1.1 Ši politika nustato saugaus debesijos paslaugų naudojimo organizacijoje reikalavimus. Ji užtikrina, kad debesijoje tvarkomi ar saugomi duomenys būtų apsaugoti, prieiga būtų kontroliuojama, o rizika valdoma atsakingai.

1.2 Ji padeda MVĮ vykdyti teisinius įsipareigojimus ir atitikti klientų lūkesčius dėl jautrios informacijos apsaugos, duomenų nutekėjimo prevencijos ir veiksmingo rizikų, susijusių su debesijos aplinkoje teikiamomis paslaugomis, valdymo, nereikalaujant įmonių grupės masto infrastruktūros.

1.3 Ši politika padeda užtikrinti ISO/IEC 27001 sertifikavimą, atitiktį ES BDAR ir tiekimo grandinės užtikrinimą, taikant nuoseklią visų trečiųjų šalių debesijos paslaugų valdyseną.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 bet kuriai debesijos aplinkoje veikiančiai paslaugai, naudojamai organizacijos duomenims saugoti, tvarkyti ar perduoti;

2.1.2 visiems darbuotojams, rangovams ir paslaugų teikėjams, naudojantiems debesijos priemones organizacijos vardu;

2.1.3 mokamoms ir nemokamoms debesijos paslaugoms, įskaitant el. pašto platformas, dokumentų bendrinimo sprendimus, SaaS priemones, atsarginių kopijų platformas, vaizdo konferencijų sprendimus ir klientų platformas;

2.1.4 bet kuriam įrenginiui (staliniam kompiuteriui, mobiliajam įrenginiui, planšetei), kuriuo per debesijos taikomąsias programas pasiekiama organizacijos informacija.

2.2 Tai apima, bet tuo neapsiriboja:

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 debesijos aplinkoje veikiančias atsarginių kopijų kūrimo ir atkūrimo po incidento priemones;

2.2.5 bendrinamus aplankus ar taikomąsias programas, naudojamas sąskaitų išrašymui, projektų valdymui ar komunikacijai su klientais.

3. Tikslai

3.1 Užkirsti kelią nesankcionuotam arba didelės rizikos nepatvirtintų debesijos paslaugų naudojimui.

3.2 Užtikrinti, kad jautrūs ar reglamentuojami duomenys, saugomi debesijoje, būtų apsaugoti taikant tinkamas technines ir administracines kontrolės priemones.

3.3 Nustatyti aiškius vaidmenis, susijusius su debesijos paslaugų tvirtinimu, konfigūravimu, stebėsena ir eksploatacijos nutraukimu.

3.4 Kontroliuoti duomenų srautus ir užtikrinti saugojimo, ištrynimo bei privatumo įsipareigojimų vykdymą debesijoje saugomai informacijai.

3.5 Mažinti priklausomybę nuo asmeninių paskyrų ar neapskaitomų priemonių, reikalaujant patvirtinimo visoms verslo tikslais naudojamoms debesijos sistemoms.

3.6 Atitikti ISO/IEC 27001:2022, ES BDAR, NIS2 direktyvos ir DORA reglamento reikalavimus, susijusius su išorinių priklausomybių nuo debesijos paslaugų valdymu.

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas (GM)

4.1.1 tvirtina visų naujų debesijos paslaugų naudojimą;

4.1.2 peržiūri rizikas, susijusias su debesijos paslaugų teikėjais ir paslaugų tipais;

4.1.3 užtikrina politikos taikymą ir prižiūri sprendimus dėl išimčių.

4.2 Išorės IT paslaugų teikėjas arba techninės pagalbos funkciją vykdantis asmuo

4.2.1 vertina ir įgyvendina saugią debesijos paslaugų konfigūraciją;

4.2.2 atlieka paskyrų parengimą, įdiegia paskyrų ir prieigos kontrolės priemones bei atsargines kopijas;

4.2.3 stebi slaptažodžių, daugiaveiksnio autentifikavimo (MFA) ir saugumo nustatymų reikalavimų laikymąsi.

[... 4.3–8 skyriai nėra įtraukti į šią peržiūrą. Įsigykite visą dokumentą, kad pasiektumėte visą turinį. ...]

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Ši politika turi būti peržiūrima ne rečiau kaip kartą per metus Generalinio vadovo, bendradarbiaujant su išorės IT paslaugų teikėju.

9.2 Formali peržiūra taip pat turi būti atliekama:

9.2.1 po su debesijos paslaugomis susijusio saugumo incidento (pvz., saugumo pažeidimo, duomenų praradimo);

9.2.2 įdiegus naują pagrindinę debesijos platformą;

9.2.3 pasikeitus teisiniams ar reguliaciniams reikalavimams (pvz., atnaujinus ES BDAR, NIS2 direktyvą ar DORA reglamentą);

9.2.4 jei stebėsenos veikla atskleidžia netinkamą naudojimą ar naujas rizikas.

9.3 GM turi užtikrinti, kad:

9.3.1 Debesijos paslaugų registras būtų atnaujintas, įtraukiant naujas arba eksploatacijos nutrauktas paslaugas;

9.3.2 teisiniai ir privatumo reikalavimai būtų toliau vykdomi;

9.3.3 apie visus pakeitimus būtų informuojami atitinkami naudotojai ir suinteresuotosios šalys.

9.4 Archyvuotos versijos turi būti saugomos saugiai, o senesnės politikos versijos tvarkomos pagal organizacijos P14S – Duomenų saugojimo ir sunaikinimo politiką.

10. Susijusios politikos ir sąsajos

10.1 Ši politika turi būti taikoma kartu su šiomis MVĮ pritaikytomis informacijos saugumo politikomis:

10.1.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: apibrėžia atskaitomybę už debesijos paslaugų tvirtinimą ir santykių su paslaugų teikėjais valdymą.

10.1.2 P4S – Prieigos kontrolės politika: palaiko saugaus prisijungimo, seansų valdymo ir prieigos teisių atšaukimo praktikas, reikalingas debesijos platformoms.

10.1.3 P14S – Duomenų saugojimo ir sunaikinimo politika: nustato, kaip debesijos aplinkoje esantys duomenys yra kopijuojami atsarginėse kopijose, saugomi ir ištrinami laikantis teisinių įsipareigojimų.

10.1.4 P17S – Duomenų apsaugos ir privatumo politika: užtikrina, kad bet kurie debesijos paslaugose saugomi asmens duomenys būtų tvarkomi pagal ES BDAR principus.

10.1.5 P30S – Reagavimo į incidentus politika: nustato struktūruotas reagavimo į debesijos saugumo incidentus procedūras, įskaitant įrodymų rinkimą ir išorinį pranešimą.

10.2 Kartu šios politikos užtikrina, kad debesijos paslaugų naudojimas būtų saugus, atitiktų reikalavimus ir būtų veiklos požiūriu atsparus.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8.1 punktas – reikalauja, kad organizacijos įgyvendintų operacines duomenų tvarkymo kontrolės priemones, įskaitant tas, kurios susijusios su debesijos aplinkoje veikiančiomis sistemomis.

11.2 ISO/IEC 27002

11.2.1 Kontrolė 5.23 – nustato valdysenos reikalavimus debesijos paslaugų ir trečiųjų šalių SaaS priemonių naudojimui.

11.2.2 Kontrolė 5.24 – reikalauja apibrėžtos debesijos naudojimo politikos, suderintos su rizikos ir reguliaciniais reikalavimais.

11.2.3 Kontrolė 5.25 – reikalauja, kad organizacijos užtikrintų, jog saugumo kontrolės priemonės debesijos aplinkose atitiktų organizacijos poreikius.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 – reikalauja formalių naudojimo politikų išorės sistemoms, tokioms kaip debesijos paslaugos.

11.3.2 SC-12, SC-13 – apima šifravimą perduodamiems ir saugomiems duomenims debesijos aplinkose.

11.3.3 SR-5 – apima su debesijos paslaugomis ir trečiosiomis šalimis susijusias tiekimo grandinės rizikos kontrolės priemones.

11.4 ES BDAR (2016/679)

11.4.1 28 straipsnis – reikalauja, kad debesijos paslaugų teikėjai, veikiantys kaip duomenų tvarkytojai, laikytųsi privalomų sutartinių įsipareigojimų.

11.4.2 32 straipsnis – nustato technines ir organizacines priemones debesijos aplinkoje vykdomam duomenų tvarkymui.

11.4.3 V skyrius – draudžia nesankcionuotus tarptautinius debesijoje saugomų asmens duomenų perdavimus.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21 straipsnio 2 dalies f ir i punktai – reikalauja, kad esminiai ir svarbūs subjektai įgyvendintų tinkamas politikas debesijos paslaugų saugumui ir tiekimo grandinės kontrolei.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 5 straipsnio 2 dalis – reikalauja, kad finansų sektoriaus MVĮ integruotų debesijos saugumą į savo IRT rizikos valdymo sistemas.

11.6.2 28 straipsnis – nustato kritinių trečiųjų šalių IRT paslaugų teikėjų, įskaitant debesijos paslaugų teikėjus, priežiūros taisykles.

11.7 COBIT 2019

11.7.1 DSS01 – „Valdyti operacijas“ apima debesijos paslaugų operacinį vientisumą.

11.7.2 DSS05 – „Valdyti saugumo paslaugas“ apima debesijai skirtas apsaugos ir stebėsenos priemones.

11.7.3 BAI04 – „Valdyti prieinamumą ir pajėgumus“ užtikrina veiklos tęstinumą ir našumą debesijos aplinkose.