					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P27					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	Komentaras
ISO/IEC 27001:2022	8 skyrius	Debesijos paslaugų operacinio planavimo ir kontrolės reikalavimai.
ISO/IEC 27002:2022	Kontrolės priemonės 5.23–5.25	Debesijos paslaugų naudojimo, politikos ir saugumo reikalavimai.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12–SC-28, SR-5	Išorinių sistemų naudojimas, sutartiniai ir techniniai reikalavimai, kriptografinės apsaugos priemonės, tiekimo grandinės apsauga.
ES BDAR	28, 32 straipsniai, V skyrius	Debesijos duomenų tvarkytojų reikalavimai, tvarkymo saugumas, duomenų perdavimas.
ES NIS2 direktyva	21 straipsnio 2 dalies f ir i punktai	Trečiųjų šalių rizikos ir tiekimo grandinės reikalavimai.
ES DORA reglamentas	5 straipsnio 2 dalis, 28 straipsnis	IRT ir trečiųjų šalių (debesijos) priežiūra finansų sektoriaus subjektams.
COBIT 2019	BAI04, DSS01, DSS05	Debesijos paslaugų prieinamumas, operacijų ir saugumo valdymas.

1. Tikslas

1.1 Ši politika nustato organizacijoje privalomus saugaus, atitiktį užtikrinančio ir atsakingo debesijos paslaugų naudojimo reikalavimus visiems infrastruktūros kaip paslaugos (IaaS), platformos kaip paslaugos (PaaS) ir programinės įrangos kaip paslaugos (SaaS) teikimo modeliams.

1.2 Šios politikos tikslas – užtikrinti, kad debesijos paslaugos būtų diegiamos ir valdomos taip, kad būtų apsaugotas informacijos išteklių konfidencialumas, vientisumas ir prieinamumas, laikantis reguliacinių, teisinių ir sutartinių įsipareigojimų.

1.3 Joje apibrėžiamos kontrolės priemonės, skirtos debesijos rizikai valdyti, duomenims apsaugoti, paslaugų teikėjų atitikčiai stebėti ir nesankcionuotam naudojimui užkardyti. Ji taip pat remia verslo inovacijas naudojant debesijos platformas, derinant saugumą, veiklos patikimumą ir kaštų efektyvumą.

2. Taikymo sritis

2.1 Ši politika taikoma visiems darbuotojams, rangovams, trečiųjų šalių paslaugų teikėjams ir išorės konsultantams, kurie organizacijos vardu inicijuoja, konfigūruoja, pasiekia, administruoja ar naudoja debesijos paslaugas.

2.2 Ji taikoma visoms aplinkoms, kuriose tvarkomi organizacijos duomenys arba darbo krūviai, įskaitant:

2.2.1 viešosios, privačiosios, hibridinės ir bendruomeninės debesijos diegimo modelius

2.2.2 visus debesijos paslaugų modelius (IaaS, PaaS, SaaS)

2.2.3 kelių debesijos paslaugų teikėjų ir federuotąsias architektūras

2.2.4 neleistiną IT (shadow IT) arba asmeninių debesijos paskyrų naudojimą verslo tikslais

2.3 Ji apima visus duomenų klasifikavimo lygius ir taikoma tiek vidaus sistemoms, tiek tiekėjų talpinamoms platformoms, kuriose saugomi arba tvarkomi organizacijai priklausantys ar reglamentuojami duomenys.

3. Tikslai

3.1 Užtikrinti saugų ir nuoseklų debesijos technologijų naudojimą, taikant aiškiai apibrėžtas naudojimo gaires, bazinius saugumo reikalavimus ir valdysenos vaidmenis.

3.2 Sumažinti su debesijos paslaugomis susijusią operacinę ir reguliacinę riziką, įskaitant neteisėtą prieigą, duomenų saugumo pažeidimus, netinkamą konfigūraciją, neatitiktį ir paslaugų sutrikimus.

3.3 Užtikrinti saugumo ir privatumo reikalavimų taikymą visiems debesijos paslaugų teikėjams ir tikrinti atitiktį pagal sutartines nuostatas, vertinimus ir audito teises.

3.4 Sudaryti sąlygas mastelį palaikančiam ir atspariam debesijos paslaugų diegimui, nebloginant saugumo būklės, nepažeidžiant teisinių reikalavimų ir veiklos tęstinumo.

3.5 Suderinti debesijos valdyseną ir naudojimą su organizacijos ISVS, teisiniais įsipareigojimais (pvz., ES BDAR, DORA reglamentu), sektoriaus gairėmis ir pramonėje pripažintomis gerosiomis praktikomis (pvz., NIST, COBIT).

4. Vaidmenys ir atsakomybės

4.1 Vadovybė

4.1.1 Tvirtina Debesijos paslaugų naudojimo politiką ir strateginį debesijos diegimo veiksmų planą.

4.1.2 Peržiūri ir tvirtina didelės rizikos išimtis nuo standartinių debesijos valdysenos reikalavimų.

4.1.3 Užtikrina, kad debesijos iniciatyvoms būtų skiriamas pakankamas finansavimas, priežiūra ir integracija į organizacijos rizikos valdymo sistemas.

4.2 Informacijos saugumo vadovas (CISO)

4.2.1 Valdo šią politiką ir organizacijos Debesijos paslaugų registrą.

4.2.2 Tvirtina naujų debesijos paslaugų teikėjų įtraukimą, remdamasis deramu patikrinimu ir rizikos vertinimu.

4.2.3 Peržiūri paslaugų teikėjų atitikties dokumentaciją ir patvirtina atitiktį saugumo reikalavimams.

[... 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 bent kartą per metus ir prireikus atnaujinama, kad būtų užtikrintas nuolatinis suderinamumas su:

9.1.1 kintančiais teisiniais ir reguliaciniais reikalavimais (pvz., ES BDAR, NIS2 direktyva, DORA reglamentu)

9.1.2 ISO/IEC 27001 ar ISO/IEC 27002 standartų pakeitimais

9.1.3 organizacijos debesijos architektūros, rizikos aplinkos ar paslaugų portfelio pokyčiais

9.1.4 incidentų tyrimais, audito rezultatais ar įgyta patirtimi iš operacinio naudojimo

9.2 CISO atsako už peržiūros inicijavimą ir susijusių suinteresuotųjų šalių sukvietimą, įskaitant:

9.2.1 Debesijos saugumo architektą

9.2.2 teisinę ir atitikties komandą

9.2.3 pirkimų ir tiekėjų valdytojus

9.2.4 paslaugų savininkus ir IT operacijų atstovus

9.3 Visi atnaujinimai turi būti:

9.3.1 valdomi taikant versijų kontrolę ir datuojami

9.3.2 tvirtinami vadovybės

9.3.3 perduodami susijusioms šalims, įskaitant darbuotojus, rangovus ir trečiąsias šalis

9.3.4 archyvuojami pagal vidaus dokumentacijos politikas

9.4 Tarpinės peržiūros gali būti inicijuojamos dėl:

9.4.1 naujų CSP paslaugų įtraukimų arba didelės apimties migracijų

9.4.2 naujai atsirandančių grėsmių debesijos infrastruktūrai

9.4.3 esminių sutartinių, teisinių ar sektoriaus įsipareigojimų pokyčių

10. Susijusios politikos ir sąsajos

10.1 Ši politika yra glaudžiai susijusi su toliau nurodytomis vidaus politikomis ir nuo jų priklauso:

10.1.1 P1 – Informacijos saugumo politika: nustato bendruosius saugaus sistemų ir paslaugų veikimo principus, kuriuos ši politika taiko debesijos kontekste.

10.1.2 P5 – Pakeitimų valdymo politika: visi debesijos konfigūracijos pakeitimai turi atitikti P5 nustatytas pakeitimų kontrolės procedūras.

10.1.3 P13 – Duomenų klasifikavimo ir ženklinimo politika: nustato, kaip duomenys vertinami prieš perkeliant juos į debesiją ir kaip taikomos tokios kontrolės priemonės kaip šifravimas ir duomenų buvimo vietos reikalavimai.

10.1.4 P18 – Kriptografinių kontrolės priemonių politika: nustato šifravimo, raktų valdymo ir kriptografinių algoritmų naudojimo standartus, kurie tiesiogiai taikomi debesijos paslaugų konfigūracijoms.

10.1.5 P22 – Žurnalų tvarkymo ir stebėsenos politika: nustato žurnalų rinkimo, saugojimo ir analizės reikalavimus, kurie turi būti taikomi debesijos aplinkose.

10.1.6 P30 – Reagavimo į incidentus politika: apibrėžia eskalavimo, lokalizavimo ir taisomųjų veiksmų procedūras su debesija susijusiems saugumo įvykiams.

10.1.7 P33 – Audito ir atitikties stebėsenos politika: remia pasirengimą auditui ir nuolatinį užtikrinimą, kad debesijos kontrolės priemonės yra taikomos ir stebimos.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001: 8.1 skyrius – Operacinis planavimas ir kontrolė: reikalauja, kad organizacijos įgyvendintų ir valdytų procesus, reikalingus informacijos saugumo reikalavimams įvykdyti, įskaitant procesus, susijusius su debesijos aplinkomis.

11.2 ISO/IEC 27002:2022 – Kontrolės priemonės 5.23–5.25:

11.2.1 A priedo kontrolės priemonė 5.23 – Debesijos paslaugų naudojimas: reikalauja rizika grindžiamo vertinimo, formalaus patvirtinimo ir debesijos paslaugų naudojimo dokumentavimo.

11.2.2 A priedo kontrolės priemonė 5.24 – Debesijos naudojimo politika: reikalauja nustatyti ir taikyti formalią debesijos naudojimo politiką, suderintą su organizacijos poreikiais ir rizikomis.

11.2.3 A priedo kontrolės priemonė 5.25 – Debesijos paslaugų saugumas: nustato poreikį integruoti saugumą, taikyti sutartines apsaugos priemones ir stebėti debesijoje veikiančius darbo krūvius bei duomenis.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – Išorinių sistemų naudojimas: reikalauja nustatytų taisyklių ir sąlygų organizacijos ištekliams pasiekti iš išorinių arba debesijos aplinkoje veikiančių sistemų.

11.3.2 SA-9(5) – Išorinių informacinių sistemų paslaugos: nustato sutartinius saugumo reikalavimus, priežiūrą ir nuolatinę trečiųjų šalių debesijos sistemų stebėseną.

11.3.3 SC-12 iki SC-28 – Kriptografinės apsaugos priemonės, perimetro apsauga ir perdavimo vientisumas: atitinka šifravimo, tapatybės ir prieigos reikalavimus debesijoje veikiančioms paslaugoms ir perduodamiems duomenims.

11.3.4 SR-5 – Tiekimo grandinės apsauga: remia CSP, dalyvaujančių paslaugų teikime, tikrinimą ir sutartinę kontrolę.

11.4 ES BDAR (2016/679):

11.4.1 28 straipsnis – Duomenų tvarkytojo pareigos: reikalauja formalių sutarčių su debesijos paslaugų teikėjais, kad būtų užtikrintas asmens duomenų tvarkymo saugumas, konfidencialumas ir audituojamumas.

11.4.2 32 straipsnis – Tvarkymo saugumas: remia šifravimo, prieigos kontrolės, žurnalų tvarkymo ir kitų apsaugos priemonių taikymą debesijos aplinkose.

11.4.3 V skyrius – Tarptautinis duomenų perdavimas: nustato teisėto duomenų perdavimo už ES / EEE ribų reikalavimus, taikant tokias apsaugos priemones kaip standartinės sutarčių sąlygos (SCC) arba tinkamumo sprendimai.

11.5 ES NIS2 direktyva (2022/2555):

11.5.1 21 straipsnio 2 dalies f ir i punktai: reikalauja, kad subjektai valdytų rizikas, kylančias dėl trečiųjų šalių debesijos paslaugų teikėjų, ir užtikrintų skaitmeninės tiekimo grandinės vientisumą, taikydami sutartines ir technines priemones.

11.6 ES DORA reglamentas (2022/2554):

11.6.1 5 straipsnio 2 dalis – IRT rizikos valdysena: reikalauja į bendrą rizikos valdyseną integruoti IRT trečiųjų šalių riziką, įskaitant debesijos paslaugas.

11.6.2 28 straipsnis – Kritinių IRT trečiųjų šalių paslaugų teikėjų priežiūra: reikalauja, kad finansų sektoriaus subjektai stebėtų, valdytų ir teiktų informaciją apie priklausomybes nuo debesijos paslaugų teikėjų, jų saugumo būklę ir atsparumą.

11.7 COBIT 2019:

11.7.1 BAI04 – Prieinamumo ir pajėgumo valdymas: užtikrina, kad debesijos paslaugos būtų atsparios, stebimos ir atitiktų nustatytus veikimo kriterijus.

11.7.2 DSS01 – Operacijų valdymas: remia operacinę integraciją, incidentų valdymą ir bazines konfigūracijas debesijoje veikiančiose platformose.

11.7.3 DSS05 – Saugumo paslaugų valdymas: nukreipia į debesijai skirtų saugumo kontrolės priemonių įgyvendinimą, stebėseną ir incidentų prevenciją skaitmeninėse paslaugose.