					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P26S					Dokumento pavadinimas: **Trečiųjų šalių ir tiekėjų saugumo 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	Operacinės kontrolės priemonės, taikomos santykiams su trečiosiomis šalimis ir tiekėjais
ISO/IEC 27002:2022	Kontrolės priemonės 5.19–5.22	Tiekėjų saugumo kontrolės priemonės, sutartinės saugumo nuostatos, pakeitimų valdymas, stebėsena ir peržiūra
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Įsigijimas, konfigūravimas, tarpusavio sujungimo susitarimai ir išorės personalo kontrolės priemonės
ES BDAR	28, 32 straipsniai	Duomenų tvarkymo sutartys, duomenų tvarkytojų saugumo reikalavimai
ES NIS2 direktyva	21(2)(a)(b)(i), 23(1) straipsniai	Tiekimo grandinės rizikos valdymas, trečiųjų šalių paslaugų priežiūra
ES DORA reglamentas	5(1)(2), 28(1)(2) straipsniai	IRT rizikos valdymas, taikomas trečiųjų šalių paslaugų teikėjams
COBIT 2019	APO10, APO12, DSS05	Tiekėjų valdymas ir rizikos integravimas

1. Tikslas

1.1 Ši politika nustato privalomuosius saugumo reikalavimus, taikomus užmezgant, valdant ir nutraukiant santykius su trečiosiomis šalimis ir tiekėjais, kurie gauna prieigą prie organizacijos duomenų, sistemų ar paslaugų arba daro jiems poveikį.

1.2 Ji užtikrina, kad išorės paslaugų teikėjai, įskaitant IT pagalbos paslaugų teikėjus, debesijos paslaugų teikėjus, programinės įrangos kūrėjus ir verslo procesų rangovus, organizacijos turtą tvarkytų saugiai ir laikydamiesi taikomų teisės aktų bei standartų.

1.3 Ši politika mažina tokias rizikas kaip duomenų nutekėjimas, nesankcionuoti sistemų pakeitimai, reguliacinės baudos ar veiklos sutrikimai, kylantys dėl nesaugių arba netinkamai valdomų susitarimų su trečiosiomis šalimis.

2. Taikymo sritis

2.1 Ši politika taikoma visoms trečiosioms šalims, kurios:

2.1.1 teikia programinę įrangą, infrastruktūrą, prieglobos ar debesijos paslaugas;

2.1.2 gauna prieigą prie vidinių sistemų, įrenginių ar taikomųjų programų arba jas administruoja;

2.1.3 tvarko organizacijos duomenis, dokumentus ar atsargines kopijas;

2.1.4 palaiko verslo operacijas, žmogiškųjų išteklių, finansų ar klientų aptarnavimo funkcijas.

2.2 Ji taip pat taikoma:

2.2.1 vidiniams darbuotojams, dalyvaujantiems tiekėjų atrankoje, samdyme ar priežiūroje;

2.2.2 visam personalui, valdančiam tiekėjų įtraukimą, sutartis, prieigą ar peržiūras;

2.2.3 visoms sistemoms ar procesams, priklausomiems nuo trečiųjų šalių komponentų ar paslaugų.

3. Tikslai

3.1 Užtikrinti, kad visi tiekėjai atitiktų aiškiai apibrėžtus saugumo reikalavimus.

3.2 Reikalauti, kad tiekėjų sutartyse būtų nustatyti vykdytini saugumo, privatumo ir reagavimo į incidentus įpareigojimai.

3.3 Įvertinti ir dokumentuoti tiekėjų rizikas prieš pasirašant susitarimus ar suteikiant prieigą.

3.4 Vykdyti reguliarias didelės rizikos ar kritinių tiekėjų peržiūras, siekiant patvirtinti atitiktį.

3.5 Nustatyti formalų išimčių valdymo, incidentų valdymo ir sutarčių atnaujinimo procesą.

3.6 Padėti užtikrinti atitiktį ISO/IEC 27001:2022, BDAR, NIS2 direktyvos ir DORA reglamento reikalavimams, susijusiems su tiekėjų valdysena.

4. Vaidmenys ir atsakomybės

4.1 Generalinis direktorius (GD)

4.1.1 prisiima galutinę atskaitomybę už tiekėjų parinkimą ir saugumo atitiktį;

4.1.2 tvirtina su tiekėjais susijusias sutartis, išimtis ir eskalavimą;

4.1.3 vykdo priežiūrą reagavimo į incidentus ir sprendimų priėmimo srityse, kai tiekėjai nevykdo nustatytų pareigų.

4.2 Išorės IT paslaugų teikėjas arba vidinis saugumo kontaktinis asmuo

4.2.1 vertina tiekėjų prašomą techninę prieigą;

4.2.2 įgyvendina prieigos kontrolės taisykles, peržiūri žurnalus ir tikrina saugų duomenų tvarkymą;

4.2.3 peržiūri saugumo kontrolės priemonių, sertifikatų ar audito rezultatų įrodymus, kai taikoma.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Šią politiką bent kartą per metus turi peržiūrėti Generalinis direktorius, dalyvaujant IT paslaugų teikėjui arba tiekėjų valdytojui.

9.2 Politika taip pat turi būti peržiūrėta:

9.2.1 po bet kokio reikšmingo teisinio, reguliacinio ar sutartinių įpareigojimų pokyčio;

9.2.2 po su tiekėju susijusio saugumo incidento ar audito išvados;

9.2.3 įtraukiant naujas tiekėjų kategorijas (pvz., kritines SaaS platformas).

9.3 Visi atnaujinimai turi būti:

9.3.1 dokumentuoti su versijų istorija ir pagrindimu;

9.3.2 patvirtinti Generalinio direktoriaus;

9.3.3 perduoti atitinkamiems vidiniams darbuotojams ir tiekėjų valdytojams;

9.3.4 saugomi kartu su ankstesnėmis versijomis pagal P14S – Duomenų saugojimo ir sunaikinimo politiką.

10. Susijusios politikos ir sąsajos

10.1 Šios politikos veiksmingumas priklauso nuo koordinavimo su šiomis MVĮ informacijos saugumo politikomis:

10.1.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: nustato atskaitomybę už tiekėjų priežiūrą ir sutarčių sąlygų taikymą.

10.1.2 P4S – Prieigos kontrolės politika: nustato prieigos ribojimo taisykles, kurios turi būti taikomos tiekėjams suteikiant sistemų prieigą.

10.1.3 P17S – Duomenų apsaugos ir privatumo politika: užtikrina, kad tiekėjai, tvarkantys asmens duomenis, laikytųsi duomenų apsaugos principų ir teisinių reikalavimų.

10.1.4 P14S – Duomenų saugojimo ir sunaikinimo politika: taikoma visiems duomenims ar įrašams, kurie perduodami tiekėjams arba jų saugomi, ir reglamentuoja saugų sunaikinimą po sutarties nutraukimo.

10.1.5 P30S – Reagavimo į incidentus politika: apibrėžia, kaip reaguoti, kai tiekėjas sukelia saugumo incidentą arba jame dalyvauja, įskaitant eskalavimo ir įrodymų tvarkymo procedūras.

10.2 Šios politikos kartu užtikrina, kad tiekėjų rizika būtų valdoma per visą sutarties gyvavimo ciklą.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8.1 skyrius – reikalauja įgyvendinti operacines kontrolės priemones, įskaitant tas, kurios taikomos santykiams su trečiosiomis šalimis ir tiekėjais.

11.2 ISO/IEC 27002

11.2.1 Kontrolės priemonė 5.19 – užtikrina, kad tiekėjų saugumo priemonės būtų suderintos su organizacijos reikalavimais.

11.2.2 Kontrolės priemonė 5.20 – reikalauja formalių susitarimų, apimančių saugumo sąlygas, atsakomybes ir įpareigojimus pažeidimo atveju.

11.2.3 Kontrolės priemonė 5.21 – valdo tiekėjų paslaugų pakeitimus, kurie gali paveikti saugumo būklę.

11.2.4 Kontrolės priemonė 5.22 – reikalauja tiekėjų paslaugų ir atitikties stebėsenos bei peržiūros.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – reglamentuoja išorės sistemų ir paslaugų įsigijimą, reikalaudamas rizikos vertinimų ir aiškiai apibrėžtų reikalavimų.

11.3.2 SA-10 – valdo konfigūravimo ir pakeitimų procedūras, susijusias su trečiųjų šalių administruojamomis sistemomis.

11.3.3 CA-3 – reikalauja tarpusavio sujungimo susitarimų sistemoms, susijusioms su išorės subjektais.

11.3.4 PS-7 – nustato išorės personalo patikrą ir atskaitomybę.

11.4 ES BDAR (2016/679)

11.4.1 28 straipsnis – reikalauja duomenų tvarkymo sutarčių su tiekėjais, veikiančiais kaip duomenų tvarkytojai.

11.4.2 32 straipsnis – nustato pareigą visiems duomenų tvarkytojams taikyti tinkamas technines ir organizacines saugumo priemones.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21(2)(a), (b), (i) straipsniai – nustato IRT tiekimo grandinės rizikos valdymo ir trečiųjų šalių kontrolės priemonių reikalavimus.

11.5.2 23(1) straipsnis – reikalauja dokumentuotos trečiųjų šalių paslaugų priežiūros esminiams ir svarbiems subjektams.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 5(1) straipsnis – reikalauja IRT rizikos valdymo sistemos, apimančios visus kritinius trečiųjų šalių paslaugų teikėjus.

11.6.2 5(2) straipsnis – nustato sutartines ir operacines kontrolės priemones IRT paslaugų priklausomybėms.

11.6.3 28(1), (2) straipsniai – nustato finansų sektoriaus IRT trečiųjų šalių rizikos priežiūros taisykles.

11.7 COBIT 2019

11.7.1 APO10 – „Tiekėjų valdymas“ apibrėžia tiekimo kontrolės priemones ir santykių valdymo reikalavimus.

11.7.2 APO12 – „Rizikos valdymas“ integruoja tiekėjų riziką į organizacijos rizikos valdyseną.

11.7.3 DSS05 – „Saugumo paslaugų valdymas“ taikomas valdomoms trečiųjų šalių ir išorinių paslaugų teikėjų paslaugoms.