					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P26					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 teisės aktais

Standartas / reglamentas	Skyrius / straipsnis	Komentaras
ISO/IEC 27001:2022	8 skyrius	Operacijų planavimas ir valdymas: reikalauja formalių kontrolės priemonių trečiųjų šalių paslaugoms, darančioms poveikį ISVS
ISO/IEC 27002:2022	Kontrolės priemonės 5.19–5.22	Politikos ir procedūros tiekėjų santykiams; tiekėjų rizikos valdymas; tiekėjų paslaugų teikimo valdymas; tiekėjų stebėsena ir peržiūra
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Išorinių sistemų paslaugos; kūrėjų konfigūracijos valdymas; sistemų tarpusavio sujungimai; trečiųjų šalių personalo saugumas
ES BDAR	28, 32, 33 straipsniai	Tvarkytojo pareigos, tvarkymo saugumas, pranešimas apie asmens duomenų saugumo pažeidimą
ES NIS2 direktyva	21 straipsnio 2 dalies e–f punktai	Rizika grindžiamas tiekėjų valdymas ir saugumo priežiūra
ES DORA reglamentas	28, 30 straipsniai	IRT trečiųjų šalių rizika, kritinių IRT trečiųjų šalių paslaugų teikėjų priežiūra
COBIT 2019	BAI05, DSS02, MEA03	Organizacinių pokyčių įgyvendinimo valdymas; paslaugų užklausų ir incidentų valdymas; atitikties stebėsena, vertinimas ir įvertinimas

1. Tikslas

1.1 Ši politika nustato informacijos saugumo reikalavimus, skirtus saugiems santykiams su trečiųjų šalių tiekėjais ir paslaugų teikėjais nustatyti, valdyti ir palaikyti.

1.2 Ji užtikrina, kad visiems tiekėjams, turintiems prieigą prie organizacijos duomenų, sistemų ar infrastruktūros, per visą paslaugų gyvavimo ciklą būtų taikomos griežtos saugumo kontrolės priemonės, sutartinės apsaugos priemonės ir nuolatinė priežiūra.

1.3 Ši politika įgyvendina ISO/IEC 27001 A priedo 5.19–5.22 kontrolės priemones, integruodama saugumo reikalavimus į pirkimų, įtraukimo, tiekėjų deramo patikrinimo, sutarčių valdymo, paslaugų stebėsenos ir sutarčių nutraukimo procesus.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 Visiems trečiųjų šalių tiekėjams, rangovams, debesijos paslaugų teikėjams ir paslaugų organizacijoms, kurie tvarko organizacijos informacijos išteklius arba prie jų jungiasi

2.1.2 Visiems vidaus vaidmenims, dalyvaujantiems tiekėjų vertinimo, įtraukimo, sutarčių sudarymo, rizikos valdymo, stebėsenos ar sutarčių nutraukimo veiklose

2.1.3 Visiems santykiams su tiekėjais, apimantiems prieigą prie jautrių duomenų, integraciją su produkcinėmis paslaugomis arba paramą kritinėms verslo funkcijoms

2.2 Ji apima tiek tiesioginius tiekėjus, tiek jų subtiekėjus, kai taikoma, taip pat trečiųjų šalių programinę įrangą, infrastruktūrą, palaikymo ir valdomąsias paslaugas.

3. Tikslai

3.1 Užtikrinti, kad tiekėjų saugumo rizikos būtų nuosekliai nustatomos, vertinamos ir mažinamos per visą santykių gyvavimo ciklą.

3.2 Į visas tiekėjų sutartis įtraukti standartizuotus saugumo reikalavimus, įskaitant pareigas pranešti apie pažeidimus, teisę atlikti auditą ir atsakomybes už duomenų apsaugą.

3.3 Reikalauti formalaus deramo patikrinimo ir dokumentuoto rizikos vertinimo prieš pradedant bendradarbiauti su naujais tiekėjais arba atnaujinant didelės rizikos paslaugų sutartis.

3.4 Nustatyti nuolatinės tiekėjų atitikties stebėsenos mechanizmus, įskaitant veiklos vertinimus, auditus ir incidentų eskalavimą.

3.5 Valdyti tiekėjų paslaugų pakeitimus ir užtikrinti saugų bendradarbiavimo nutraukimo procesą bei duomenų grąžinimą arba sunaikinimą nutraukiant sutartį.

3.6 Suderinti trečiųjų šalių saugumo kontrolės priemones su taikomais teisės aktų ir sutartiniais įpareigojimais, įskaitant ES BDAR, NIS2 direktyvą, DORA reglamentą ir ISO/IEC 27001 standartus.

4. Vaidmenys ir atsakomybės

4.1 Vyriausiasis informacijos saugumo pareigūnas

4.1.1 Atsako už šią politiką ir užtikrina jos suderinamumą su bendra ISVS, rizikos valdymo ir atitikties strategija.

4.1.2 Tvirtina tiekėjų klasifikavimo lygius, saugumo peržiūrų rezultatus ir didelės rizikos išimtis.

4.1.3 Dalyvauja eskaluojant reikšmingus tiekėjų incidentus ir derantis dėl kritinių paslaugų sutarčių.

4.2 Pirkimų ir tiekėjų valdymo funkcija

4.2.1 Užtikrina, kad į visas naujas ir atnaujinamas tiekėjų sutartis būtų įtrauktos patvirtintos saugumo ir duomenų apsaugos nuostatos.

4.2.2 Prižiūri centralizuotą tiekėjų registrą ir koordinuoja veiklą su teisine bei atitikties funkcijomis dėl trečiųjų šalių rizikos dokumentavimo.

4.2.3 Inicijuoja tiekėjų įtraukimo procesus ir užtikrina jų suderinamumą su ikisutartiniais saugumo vertinimais.

[... 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 arba anksčiau, jei įvyksta:

9.1.1 Esminiai pirkimų strategijos arba tiekėjų ekosistemos pokyčiai

9.1.2 Teisės aktų ar reguliacinės sistemos atnaujinimai (pvz., DORA reglamentas, ES BDAR)

9.1.3 Reikšmingi trečiųjų šalių incidentai, duomenų saugumo pažeidimai arba audito neatitiktys

9.1.4 Rizikos vertinimų ar išorės sertifikavimo įstaigų išvados

9.2 Už peržiūros procesą bendrai atsako Vyriausiasis informacijos saugumo pareigūnas, pirkimų, teisės ir rizikos valdymo funkcijos.

9.3 Visi politikos pakeitimai turi būti dokumentuojami ISVS dokumentų kontrolės registre, valdomi pagal versijų kontrolę ir perduodami atitinkamoms suinteresuotosioms šalims per tiekėjų valdysenos kanalus ir darbuotojų informuotumo didinimo programas.

9.4 Pakeistos versijos turi būti archyvuojamos ne trumpiau kaip trejus metus, siekiant užtikrinti atsekamumą ir teisinę atitiktį.

10. Susijusios politikos ir sąsajos

10.1 P1 – Informacijos saugumo politika. Nustato bendrą įsipareigojimą saugiai vykdyti visas organizacijos operacijas, įskaitant priklausomybę nuo trečiųjų šalių tiekėjų ir išorės paslaugų teikėjų.

10.2 P6 – Rizikos valdymo politika. Reglamentuoja trečiųjų šalių santykių rizikų nustatymą, vertinimą ir mažinimą, įskaitant iš tiekėjų ekosistemų kylančią paveldėtą ar sisteminę riziką.

10.3 P17 – Duomenų apsaugos ir privatumo politika. Taikoma visiems tiekėjams, tvarkantiems asmens duomenis, ir reikalauja tinkamų sutartinių nuostatų, duomenų perdavimo apsaugos priemonių bei privatumo pagal projektavimą principų.

10.4 P4 – Prieigos kontrolės politika. Reguliuoja, kaip trečiųjų šalių personalui suteikiama prieiga prie organizacijos sistemų, užtikrinant vaidmenimis grindžiamus leidimus, sesijų kontrolę ir prieigos teisių atšaukimo procedūras.

10.5 P22 – Žurnalų tvarkymo ir stebėsenos politika. Reikalauja, kad tiekėjų prieiga prie sistemų būtų stebima, registruojama ir peržiūrima, ypač aplinkose, kuriose vykdoma privilegijuota arba į duomenis orientuota veikla.

10.6 P30 – Reagavimo į incidentus politika. Nustato eskalavimo procedūras ir pranešimo apie pažeidimus reikalavimus tiekėjų sukeltų saugumo įvykių arba bendrų tyrimų, susijusių su trečiųjų šalių sistemomis, atvejais.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001: 8.1 skyrius – Operacijų planavimas ir valdymas: reikalauja formalių kontrolės priemonių trečiųjų šalių paslaugoms, darančioms poveikį ISVS.

11.2 ISO/IEC 27002:2022 – kontrolės priemonės 5.19–5.22:

11.2.1 A priedo 5.19 kontrolės priemonė – Politikos ir procedūros tiekėjų santykiams: nustato pareigą taikyti kontrolės priemones tiekėjų sąveikai valdyti.

11.2.2 A priedo 5.20 kontrolės priemonė – Tiekėjų rizikos valdymas: orientuota į tiekėjų saugumo būklės nustatymą, vertinimą ir nuolatinę priežiūrą.

11.2.3 A priedo 5.21 kontrolės priemonė – Tiekėjų paslaugų teikimo valdymas: reikalauja veiklos ir saugumo suderinamumo su sutartiniais lūkesčiais.

11.2.4 A priedo 5.22 kontrolės priemonė – Tiekėjų stebėsena ir peržiūra: sustiprina nuolatinio trečiųjų šalių atitikties patvirtinimo ir pakartotinio vertinimo poreikį.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SA-9 – Išorinių sistemų paslaugos: apibrėžia saugumo ir rizikos reikalavimus sistemoms, kurias eksploatuoja išorės subjektai.

11.3.2 SA-10 – Kūrėjų konfigūracijos valdymas: taikoma, kai trečiosios šalys teikia programinę įrangą ar aplinkas.

11.3.3 CA-3 – Sistemų tarpusavio sujungimai: reikalauja priežiūros ir susitarimų dėl duomenų srautų tarp subjektų.

11.3.4 PS-7 – Trečiųjų šalių personalo saugumas: užtikrina, kad rangovai ir tiekėjų darbuotojai būtų tinkamai tikrinami ir stebimi.

11.4 ES BDAR (2016/679):

11.4.1 28 straipsnis – Tvarkytojo pareigos: reikalauja rašytinių susitarimų su duomenų tvarkytojais, įskaitant technines ir organizacines priemones (TOM).

11.4.2 32 straipsnis – Tvarkymo saugumas: nustato pareigą tiek duomenų valdytojams, tiek duomenų tvarkytojams taikyti tinkamas apsaugos priemones.

11.4.3 33 straipsnis – Pranešimas apie asmens duomenų saugumo pažeidimą: reikalauja, kad tiekėjai pažeidimo atveju praneštų nedelsdami.

11.5 ES NIS2 direktyva (2022/2555):

11.5.1 21 straipsnio 2 dalies e–f punktai: reikalauja rizika grindžiamo tiekėjų valdymo ir saugumo priežiūros, ypač esminių ir svarbių subjektų skaitmeninėse tiekimo grandinėse.

11.6 ES DORA reglamentas (2022/2554):

11.6.1 28 straipsnis – IRT trečiųjų šalių rizika: nustato pareigas dėl rizikos vertinimo, sutartinių saugumo nuostatų ir pasitraukimo strategijų finansinių paslaugų teikėjams.

11.6.2 30 straipsnis – Kritinių IRT trečiųjų šalių paslaugų teikėjų priežiūra: nustato sustiprintos stebėsenos ir priežiūros lūkesčius pagrindiniams tiekėjams.

11.7 COBIT 2019:

11.7.1 BAI05 – Organizacinių pokyčių įgyvendinimo valdymas: užtikrina, kad perėjimai tarp tiekėjų būtų valdomi saugiai.

11.7.2 DSS02 – Paslaugų užklausų ir incidentų valdymas: taikoma tiekėjų praneštoms problemoms ir incidentų valdymo integracijai.

11.7.3 MEA03 – Atitikties stebėsena, vertinimas ir įvertinimas: sustiprina tiekėjų veiklos matavimo ir atitikties stebėsenos svarbą.