					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P06					Dokumento pavadinimas: **Rizikos valdymo 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 taikytinais standartais ir reglamentavimo reikalavimais

Standartas / reglamentavimas	Punktas / straipsnis	Pastaba
ISO/IEC 27001:2022	6.1, 8.32, 10 punktai	Rizikų identifikavimo ir valdymo pagrindas, integravimas į pakeitimų valdymą, nuolatinis tobulinimas
ISO/IEC 27005:2024	Visa rizikos gyvavimo ciklo metodika	Visas rizikos valdymo procesas pagal standartą
ISO 31000:2018	Rizikos valdymo principai ir sistema	Sistemoje taikomi rizikos valdymo principai
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Gairės ir struktūra rizikos vertinimams, pakopinė rizikos valdysena
ES BDAR	24, 25, 32 straipsniai	Duomenų apsaugos rizikos procesai ir kontrolės priemonės
ES NIS2 direktyva	21 straipsnio 2 dalies a–d punktai	Rizikos ir saugumo vertinimo pareigos
ES DORA reglamentas	5, 6 straipsniai	IRT rizikos valdymas ir veiklos atsparumas
COBIT 2019	APO12, MEA	Rizikos valdymo struktūra ir priežiūra

1. Tikslas

1.1 Ši politika nustato vieningą ir formalizuotą sistemą, skirtą informacijos saugos rizikų identifikavimui, analizei, vertinimui, tvarkymui, stebėsenai ir peržiūrai visoje organizacijoje.

1.2 Ji užtikrina nuoseklų rizika grindžiamų principų taikymą, siekiant apsaugoti informacijos turto konfidencialumą, vientisumą ir prieinamumą pagal ISO/IEC 27001:2022 6.1 punktą ir ISO 31000:2018.

1.3 Ši politika integruoja informacijos saugos rizikos valdymą į organizacijos sprendimų priėmimo procesus, kad būtų pasiekti vidaus strateginiai tikslai ir įvykdyti išoriniai reglamentavimo reikalavimai.

2. Taikymo sritis

2.1 Ši politika taikoma visiems organizaciniams vienetams, verslo procesams, sistemoms, personalui ir bendradarbiavimui su trečiosiomis šalimis, susijusiems su informacijos turto tvarkymu, kūrimu, saugojimu ar valdymu.

2.2 Taikymo sritis apima fizinį, skaitmeninį ir debesijos aplinkoje talpinamą turtą, įskaitant struktūrizuotus ir nestruktūrizuotus duomenis, taikomąsias programas, infrastruktūrą, tinklus ir paslaugas.

2.3 Ji apima informacijos saugos rizikas strateginiu, operaciniu, projektiniu ir techniniu lygmenimis ir yra privaloma visiems darbuotojams, rangovams ir paslaugų teikėjams, dalyvaujantiems ISVS veiklose.

2.4 Rizikos valdymas turi būti taikomas šiais atvejais:

2.4.1 diegiant naują projektą arba sistemą

2.4.1.1 atliekant reikšmingus pakeitimus (pvz., architektūros, nuosavybės, procesų)

2.4.1.2 įtraukiant tiekėjus ir sudarant susitarimus su trečiosiomis šalimis

2.4.1.3 reaguojant į incidentus ir atliekant poincidentines peržiūras

2.4.1.4 atliekant periodines organizacines rizikos peržiūras arba auditus

3. Tikslai

3.1 Nustatyti ir taikyti pakartojamą, visos organizacijos mastu veikiantį rizikos valdymo procesą, pagrįstą ISO/IEC 27005 ir ISO 31000 metodikomis.

3.2 Užtikrinti, kad rizikos būtų identifikuojamos, analizuojamos, vertinamos ir tvarkomos taikant struktūrizuotus, atsekamumą užtikrinančius metodus, įskaitant rizikos savininkų priskyrimą ir sąsajas su kontrolės priemonėmis.

3.3 Palaikyti centralizuotą, pagal versijų valdymo principus tvarkomą Rizikų registrą ir Rizikos tvarkymo planą, atspindinčius esamą rizikos būseną, kontrolės priemonių aprėptį ir rizikos mažinimo pažangą.

3.4 Suderinti sprendimus dėl rizikos su dokumentuotu rizikos apetitu ir tolerancijos lygiais bei sudaryti sąlygas pagrįstiems valdysenos sprendimams dėl rizikos priėmimo, mažinimo, perdavimo ar vengimo.

3.5 Nuolat stebėti rizikos tendencijas ir užtikrinti rizikos valdymo priemonių veiksmingumą, kartu sudarant sąlygas aktyviems koregavimams pagal grėsmių raidą arba verslo pokyčius.

4. Vaidmenys ir atsakomybės

4.1 Aukščiausioji vadovybė / Valdyba

4.1.1 Tvirtina rizikos valdymo sistemą ir nustato priimtiną rizikos apetitą bei rizikos priėmimo slenksčius.

4.1.2 Tvirtina rizikos tvarkymo strategijas, skirtas likutinei rizikai, viršijančiai tolerancijos lygį.

4.1.3 Skiria išteklius ir užtikrina priežiūrą, reikalingą veiksmingam rizikos valdymo programos veikimui.

4.2 ISVS vadovas / rizikos pareigūnas

4.2.1 Atsako už šią politiką ir palaiko jos atitiktį ISO/IEC 27001 ir ISO/IEC 27005 standartams.

4.2.2 Vadovauja organizacijos rizikos vertinimo procesui ir tvarko Rizikų registrą bei Rizikos tvarkymo planą.

4.2.3 Užtikrina periodines peržiūras ir esminių rizikų eskalavimą aukščiausiajai vadovybei arba Informacijos saugumo valdymo komitetui (ISSC).

[... 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 ir su ja susijusi sistema turi būti peržiūrimos kasmet arba:

9.1.1 po didelio rizikos įvykio arba saugumo incidento

9.1.2 po reikšmingo organizacinio arba techninio pakeitimo

9.1.3 reaguojant į audito išvadas arba naujus reglamentavimo reikalavimus

9.2 ISVS vadovas, rizikos pareigūnas ir atitikties komanda kartu atsako už:

9.2.1 peržiūros ciklo inicijavimą

9.2.2 įvesties surinkimą iš verslo padalinių

9.2.3 procedūrų ir slenksčių peržiūrą bei atnaujinimą pagal poreikį

9.3 Visi pakeitimai turi būti:

9.3.1 tvarkomi pagal versijų valdymą ir registruojami

9.3.2 patvirtinti aukščiausiosios vadovybės

9.3.3 pranešti suinteresuotosioms šalims

9.3.4 saugomi audito saugykloje ne trumpiau kaip 5 metus

10. Susijusios politikos ir sąsajos

10.1 Ši politika yra susijusi su šiomis informacijos saugos politikomis:

10.1.1 P1 – Informacijos saugos politika: nustato bendrą saugumo valdysenos modelį, kuriame taikoma ši rizikos politika.

10.1.2 P2 – Valdysenos vaidmenų ir atsakomybių politika: apibrėžia atsakingus savininkus ir valdysenos lygius, nurodytus rizikos eskalavimo matricoje.

10.1.3 P5 – Pakeitimų valdymo politika: inicijuoja pakartotinį rizikos vertinimą infrastruktūros ir organizacinių pakeitimų atvejais.

10.1.4 P13 – Duomenų klasifikavimo ir ženklinimo politika: padeda atlikti poveikio vertinimą rizikų identifikavimo metu.

10.1.5 P33 – Audito ir atitikties stebėsenos politika: patvirtina politikos laikymąsi, įskaitant Rizikų registro išsamumą ir rizikos tvarkymo įrodymus.

11. Pamatiniai standartai ir sistemos

11.1 Ši politika yra aiškiai suderinta su toliau nurodytais standartais ir sistemomis, siekiant užtikrinti jos atitiktį tarptautinėms gerosioms praktikoms ir reglamentavimo lūkesčiams informacijos saugos rizikos valdymo srityje:

11.2 ISO/IEC 27001:

11.2.1 6.1 punktas: nustato reikalavimus rizikų ir galimybių identifikavimui, įskaitant visą informacijos saugos rizikos vertinimo ir rizikos tvarkymo gyvavimo ciklą. Ši politika įgyvendina 6.1.2 ir 6.1 punktų reikalavimus per struktūrizuotą sistemą, kuri nustato privalomus dokumentuotus rizikų identifikavimo, analizės, vertinimo, tvarkymo ir likutinės rizikos priėmimo protokolus.

11.2.2 8.32 punktas: rizika grindžiamo mąstymo integravimas į pakeitimų valdymo procesus užtikrina, kad visi reikšmingi organizaciniai pokyčiai inicijuotų formalų pakartotinį rizikos vertinimą.

11.2.3 10 punktas: nuolatinis tobulinimas užtikrinamas reguliariomis politikos peržiūromis, rizikos tendencijų analize ir SoA atnaujinimais, grindžiamais rizikos įžvalgomis.

11.3 ISO/IEC 27005:

11.3.1 Pateikia specializuotas ir išsamias gaires dėl informacijos saugos rizikos valdymo. Ši politika įgyvendina visą ISO/IEC 27005 rizikos proceso modelį: konteksto nustatymą, rizikų identifikavimą, rizikos analizę, rizikos vertinimą, rizikos tvarkymą, rizikos priėmimą, rizikos komunikavimą, stebėseną ir peržiūrą.

11.4 ISO 31000:

11.4.1 Ši politika integruoja ISO 31000 principus, tokius kaip vadovybės įsipareigojimas, integravimas į sprendimų priėmimą ir nuolatinis tobulinimas. Ji užtikrina, kad rizikos valdymas būtų integruotas į organizacijos kultūrą ir veiklą.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Suderinta su NIST gairėmis dėl rizikos vertinimų atlikimo, įskaitant grėsmių identifikavimą, pažeidžiamumų analizę, tikimybės įvertinimą ir poveikio nustatymą. Šios politikos struktūra atitinka NIST apibrėžtus rizikos vertinimo žingsnius ir juos pritaiko tiek techniniams, tiek verslo procesams.

11.6 NIST SP 800-39:

11.6.1 Palaiko organizacijos lygmens rizikos valdyseną, pabrėždama pakopinį rizikos valdymą organizacijos, misijos / verslo proceso ir informacinės sistemos lygmenimis. Ši politika užtikrina, kad rizikos savininkystė būtų aiškiai apibrėžta visais lygiais ir apimtų organizacijos lygmens rizikos tvarkymo strategijas.

11.7 ES BDAR:

11.7.1 24 straipsnis: reikalauja įgyvendinti tinkamas technines ir organizacines priemones, kad duomenų apsaugos rizikos būtų tinkamai valdomos; tai užtikrinama šioje politikoje nustatytu struktūrizuotu rizikos procesu.

11.7.2 25 straipsnis: „duomenų apsauga pagal projektavimą ir numatytuosius nustatymus“ atitinka rizikos tvarkymo integravimą į sistemų ir procesų projektavimą.

11.7.3 32 straipsnis: nustato rizika grindžiamą požiūrį į saugumo priemones; šis reikalavimas įgyvendinamas per poveikiu grindžiamą rizikos vertinimą ir kontrolės priemonių parinkimą.

11.8 ES NIS2 direktyva:

11.8.1 21 straipsnio 2 dalies a–d punktai: reikalauja, kad subjektai atliktų rizikos vertinimus, įgyvendintų rizikos analizės politikas ir užtikrintų proporcingas saugumo priemones. Ši politika šias pareigas įgyvendina taikydama nuolatinį rizikos gyvavimo ciklą ir dokumentuotą valdyseną.

11.9 ES DORA reglamentas:

11.9.1 5 straipsnis: reikalauja dokumentuotos IRT rizikos valdymo sistemos; tai visiškai apima šios politikos struktūra, įskaitant susiejimą su SoA ir KRI.

11.9.2 6 straipsnis: reikalauja integruoti rizikos valdymą į veiklos atsparumo strategijas; tai užtikrinama per rizikos eskalavimo matricas ir kritinio turto stebėseną.

11.10 COBIT 2019:

11.10.1 APO12 – Rizikos valdymas: tiesiogiai atitinka organizacijos įdiegtą struktūrizuotą rizikos valdymo metodą, vaidmenų priskyrimą, rizikos tvarkymo priemonių sekimą ir Valdybos lygmens atskaitomybę.

11.10.2 MEA01 – veiklos rezultatyvumo ir atitikties stebėsena, vertinimas ir įvertinimas: atsispindi šios politikos dėmesyje tendencijų analizei, KRI stebėsenai ir audito grįžtamojo ryšio integravimui į nuolatinio tobulinimo ciklus.