					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P06S					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 taikomais standartais ir teisės aktais

Standartas / reglamentavimas	Skyrius / straipsnis	Pastaba
ISO/IEC 27001:2022	6.1, 6.1 punktai	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1–RA-7, PM-9	
ES NIS2 direktyva	21 straipsnio 2 dalies a–d punktai	
ES DORA reglamentas	5 straipsnis	
COBIT 2019	APO12, MEA	

1. Tikslas

1.1 Ši politika nustato, kaip organizacija identifikuoja, vertina ir valdo rizikas, susijusias su informacijos sauga, veikla, technologijomis ir trečiųjų šalių paslaugomis.

1.2 Ji užtikrina, kad rizikos valdymas būtų neatsiejama planavimo, projektų įgyvendinimo, tiekėjų atrankos ir reagavimo į incidentus dalis, laikantis ISO 27001, ISO 31000 ir taikomų reglamentavimo reikalavimų.

1.3 Ši politika padeda priimti pagrįstus sprendimus, apsaugoti informacinius išteklius ir užtikrinti kritinių verslo operacijų atsparumą.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 visiems organizacijos padaliniams, sistemoms ir naudotojams;

2.1.2 visai informacijai, paslaugoms ir turtui, valdomiems organizacijos viduje arba per trečiąsias šalis;

2.1.3 visoms su rizika susijusioms veikloms, įskaitant projektų peržiūras, sistemų atnaujinimus, išorinių paslaugų įsigijimą ir atitikties reglamentavimo reikalavimams užtikrinimą.

2.2 Ji apima visas rizikų rūšis, įskaitant:

2.2.1 kibernetinio saugumo grėsmes ir sistemų pažeidžiamumus;

2.2.2 veiklos sutrikimus ir paslaugų nepasiekiamumą;

2.2.3 teisinę, atitikties ir reputacijos riziką;

2.2.4 trečiųjų šalių ir tiekimo grandinės rizikas.

2.3 Visi darbuotojai, rangovai ir paslaugų teikėjai, identifikuodami rizikas arba apie jas pranešdami, privalo laikytis šios politikos.

3. Tikslai

3.1 Integruoti paprastas ir pakartojamas rizikos vertinimo procedūras į įprastą verslo veiklą.

3.2 Identifikuoti ir prioritetizuoti rizikas, kurios gali paveikti konfidencialumą, vientisumą, prieinamumą arba teisinę atitiktį.

3.3 Priskirti savininkus ir apibrėžti rizikos tvarkymo veiksmus visoms reikšmingoms rizikoms.

3.4 Palaikyti tikslų ir aktualų Rizikų registrą, siekiant užtikrinti pasirengimą auditui ir rizikų stebėseną.

3.5 Užtikrinti vadovybės dalyvavimą tvirtinant rizikos toleranciją ir pagrindinius rizikos tvarkymo planus.

4. Vaidmenys ir atsakomybės

4.1 Generalinis direktorius

4.1.1 Nustato organizacijos rizikos apetitą ir tvirtina rizikos valdymo sistemą.

4.1.2 Tvirtina pagrindinius sprendimus dėl rizikos tvarkymo ir tam reikalingus išteklius.

4.1.3 Kiekvieną ketvirtį kartu su rizikos koordinatoriumi peržiūri svarbiausias rizikas.

4.2 Rizikos koordinatorius (arba ISVS savininkas)

4.2.1 Koordinuoja rizikos vertinimus ir prižiūri Rizikų registrą.

4.2.2 Užtikrina, kad rizikos balas, rizikos savininkystė ir rizikos tvarkymo veiksmai būtų dokumentuoti.

4.2.3 Organizuoja bent vieną formalią rizikų peržiūrą per metus.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Kasmetinė politikos peržiūra

9.1.1 Šią politiką ne rečiau kaip kartą per metus turi peržiūrėti generalinis direktorius ir rizikos koordinatorius, kad būtų užtikrintas jos aktualumas ir išsamumas.

9.2 Atnaujinimo inicijavimo kriterijai

9.2.1 Ankstesnė peržiūra ir atnaujinimas turi būti atliekami, jei:

9.2.1.1 didelis incidentas arba audito išvados atskleidžia rizikos valdymo spragas;

9.2.1.2 įdiegiami nauji verslo padaliniai, technologijos arba partnerystės;

9.2.1.3 pasikeičia reglamentavimo arba sutartiniai reikalavimai.

9.3 Versijų valdymas

9.3.1 Visi šios politikos atnaujinimai turi būti versijuojami, nurodant šiuos metaduomenis:

9.3.1.1 versijos numerį ir įsigaliojimo datą;

9.3.1.2 pakeitimų santrauką;

9.3.1.3 tvirtintoją (generalinį direktorių);

9.3.1.4 ankstesnių versijų archyvavimą audito tikslais.

9.4 Komunikavimas ir informuotumas

9.4.1 Atnaujintos politikos versijos ir pagrindiniai rizikos tvarkymo planai turi būti komunikuojami susijusiems darbuotojams. Į metinius pakartotinius mokymus turi būti įtraukti pagrindiniai informuotumo apie riziką principai.

10. Susijusios politikos ir sąsajos

10.1 Ši politika taikoma kartu su kitomis politikomis, siekiant užtikrinti visapusišką saugumo valdyseną:

10.1.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: nustato, kas atsakingas už rizikos savininkystę ir sprendimų priėmimą.

10.1.2 P5S – Pakeitimų valdymo politika: reikalauja atlikti rizikos vertinimą prieš įgyvendinant techninius ar procesų pakeitimus.

10.1.3 P17S – Duomenų apsaugos ir privatumo politika: apima reglamentavimo riziką, susijusią su asmens duomenų tvarkymu.

10.1.4 P30S – Reagavimo į incidentus politika: užtikrina, kad rizikos tvarkymas būtų tęsiamas saugumo incidentų metu ir po jų.

10.1.5 P33S – Veiklos tęstinumo politika: identifikuoja likutines rizikas ir atkūrimo priemones kritinėms paslaugoms.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001:

11.1.1 6.1 punktas – nustato formalų rizikos valdymo procesą ir rizikos tvarkymo planavimą.

11.1.2 6.1.3 punktas – reikalauja, kad organizacijos išsaugotų dokumentuotus rizikos tvarkymo planus ir patvirtinimus.

11.2 ISO/IEC 27002:

11.2.1 5.4, 5.25 kontrolės priemonės – pateikia įgyvendinimo gaires dėl rizikos savininkystės, prioritetizavimo ir gyvavimo ciklo valdymo.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1–RA-7 – apibrėžia rizikos vertinimą, reagavimo strategijas, dokumentavimą ir peržiūros mechanizmus.

11.4 PM-9 – reikalauja nuoseklios organizacijos rizikų priežiūros vadovybės lygmeniu.

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies a–d punktai – nustato privalomas rizikos vertinimo, rizikos mažinimo ir valdysenos kontrolės priemones esminiams ir svarbiems subjektams.

11.6 ES DORA reglamentas

11.6.1 5 straipsnis – reikalauja, kad reguliuojami subjektai apibrėžtų ir valdytų IRT rizikos valdymo sistemas, įskaitant identifikavimą, klasifikavimą ir reagavimą.

11.7 COBIT 2019

11.7.1 APO12 – Rizikos valdymas: integruoja riziką į strateginį ir operacinį planavimą.

11.7.2 MEA01 – Stebėti, vertinti ir nustatyti: užtikrina rizikos procesų ir veiksmų veiksmingumą bei atitiktį.