					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P02					Dokumento pavadinimas: **Valdysenos vaidmenų ir atsakomybių 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 reglamentavimo reikalavimais

Standartas / reglamentavimas	Skyrius / straipsnis	Pastaba
ISO/IEC 27001:2022	5.3 punktas; A priedo kontrolė 5	
ISO/IEC 27002:2022	Kontrolė 5	
NIST SP 800-53 Rev.5	PL-1–PL-4, PM-1–PM-13	
ES BDAR	5 straipsnio 1 dalies f punktas, 24, 37 straipsniai	
ES NIS2 direktyva	21 straipsnio 2 dalies a punktas	
ES DORA reglamentas	5 straipsnis	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Tikslas

1.1 Ši politika apibrėžia valdysenos modelį, organizacinius vaidmenis ir atsakomybes, reikalingus veiksmingam Informacijos saugumo valdymo sistemos (ISVS) veikimui užtikrinti.

1.2 Joje nustatomos aiškios atskaitomybės ribos, sprendimų priėmimo įgaliojimai ir eskalavimo keliai, siekiant užtikrinti, kad informacijos saugumas būtų integruotas visuose organizacijos lygmenyse ir suderintas su strateginiais verslo tikslais.

1.3 Ši politika įgyvendina ISO/IEC 27001:2022 5.3 punkto ir A.5.2 kontrolės reikalavimus, užtikrindama, kad su sauga susijusių veiklų atsakomybės būtų aiškiai priskirtos, dokumentuotos, perduotos ir periodiškai peržiūrimos.

1.4 Ši politika taip pat sudaro pagrindą integruotai valdysenai su kitomis sritimis, tokiomis kaip rizikos valdymas, atitiktis, IT operacijos ir teisinė funkcija.

2. Taikymo sritis

2.1 Ši politika taikoma visiems asmenims ir subjektams, dalyvaujantiems informacijos saugumo valdysenoje, vykdyme ir priežiūroje ISVS taikymo srityje. Tai apima:

2.1.1 aukščiausiąją vadovybę, vyresniąją vadovybę ir valdybos narius;

2.1.2 ISVS vadovus, vyriausiąjį informacijos saugumo pareigūną ir kontrolių savininkus;

2.1.3 procesų ir turto savininkus;

2.1.4 rangovus ir trečiųjų šalių paslaugų teikėjus, kuriems deleguotos su sauga susijusios atsakomybės.

2.2 Ji apima tiek vidines, tiek išorės paslaugų funkcijas (pvz., išorinį SOC, debesijos platformų administratorius), kai valdysenos vaidmenys yra formaliai priskirti arba apibrėžti sutartyse.

2.3 Politika taip pat taikoma organizaciniams padaliniams, departamentams ir projektų komandoms, kurios valdo arba daro įtaką saugai svarbiam turtui, sistemoms ar paslaugoms.

3. Tikslai

3.1 Užtikrinti, kad informacijos saugumo vaidmenys ir atsakomybės būtų formaliai apibrėžti, priskirti, perduoti ir dokumentuoti.

3.2 Palaikyti valdysenos modelį, kuris užtikrina pareigų atskyrimą (SoD), pašalina interesų konfliktus ir sudaro sąlygas eskaluoti neišspręstus saugumo klausimus.

3.3 Užtikrinti, kad atskaitomybė ir įgaliojimai priimti su sauga susijusius sprendimus būtų paskirstyti pagal verslo poveikį ir organizacinę struktūrą.

3.4 Nustatyti sistemą, skirtą delegavimo, vaidmenų pokyčių ir priskirtų atsakomybių peržiūros valdymui.

3.5 Suteikti užtikrinimą suinteresuotosioms šalims, įskaitant reguliuotojus, auditorius ir klientus, kad informacijos saugumo valdysena vykdoma veiksmingai ir laikantis taikomų standartų.

4. Vaidmenys ir atsakomybės

4.1 Aukščiausioji vadovybė

4.1.1 Užtikrina strateginę priežiūrą, skiria išteklius ir užtikrina ISVS tikslų suderinimą su verslo tikslais.

4.1.2 Tvirtina pagrindinę ISVS dokumentaciją, įskaitant Informacijos saugumo politiką, rizikos tvarkymo planus ir sprendimus dėl audito neatitikčių šalinimo.

4.1.3 Dalyvauja ISVS vadovybės peržiūrose ir eskaluoja sprendimus, kuriems reikalingas valdybos lygmens patvirtinimas.

4.1.4 Skatina saugumo kultūrą ir organizacijos politikų laikymąsi pagal saugumo valdysenos principus.

4.2 Informacijos saugumo valdymo komitetas (ISSC)

4.2.1 Veikia kaip tarpfunkcinis ISVS priežiūros valdysenos organas.

4.2.2 Peržiūri rizikos būklę, kontrolių veiksmingumą, audito išvadas ir strategines saugumo iniciatyvas.

4.2.3 Užtikrina koordinavimą tarp padalinių (pvz., IT, teisės, žmogiškųjų išteklių, rizikos, atitikties, operacijų).

4.2.4 Tvirtina eskalavimo slenksčius, biudžeto paskirstymą ir politikos pakeitimus, kuriems reikalingas vykdomosios vadovybės įsitraukimas.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Peržiūros grafikas

9.1.1 Ši politika turi būti peržiūrima bent kartą per metus arba įvykus bent vienai iš šių aplinkybių:

9.1.1.1 pasikeitus organizacinei struktūrai arba vykdomajai komandai;

9.1.1.2 išplėtus arba iš naujo apibrėžus ISVS taikymo sritį;

9.1.1.3 pasikeitus reglamentavimo reikalavimams, turintiems įtakos vaidmenų priskyrimui arba priežiūrai;

9.1.1.4 esant reikšmingoms audito išvadoms arba incidentams, susijusiems su valdysenos neveikimu.

9.2 Peržiūros ir tvirtinimo procesas

9.2.1 ISVS vadovas inicijuoja ir vadovauja peržiūros procesui, įskaitant suinteresuotųjų šalių nuomonės ir audito grįžtamojo ryšio surinkimą.

9.2.2 Siūlomi atnaujinimai turi būti peržiūrėti ISSC ir formaliai patvirtinti aukščiausiosios vadovybės.

9.2.3 Kiekviena versija turi būti registruojama ISVS dokumentų registre ir apimti šiuos metaduomenis:

9.2.3.1 politikos identifikatorių ir pavadinimą;

9.2.3.2 versijos numerį ir pakeitimų santrauką;

9.2.3.3 įsigaliojimo datą ir kitos peržiūros datą;

9.2.3.4 politikos savininką ir tvirtinantį asmenį;

9.2.3.5 dokumento klasifikavimo lygį;

9.2.3.6 saugojimo ir archyvavimo istoriją.

10. Susijusios politikos ir sąsajos

10.1 Ši politika turi būti aiškinama kartu su šiomis politikomis:

10.1.1 P1 – Informacijos saugumo politika: nustato bendrą saugumo programą ir apibrėžia vadovybės atsakomybes už politikos patvirtinimą ir strateginę priežiūrą.

10.1.2 P5 – Pakeitimų valdymo politika: užtikrina, kad valdysenos struktūrų, vaidmenų ar atsakomybių pakeitimams būtų taikomas dokumentuotas patvirtinimas ir rizikos peržiūra.

10.1.3 P6 – Rizikos valdymo politika: identifikuoja ir tvarko valdysenos rizikas, kylančias dėl vaidmenų konfliktų, nepriskirtų pareigų arba eskalavimo nebuvimo.

10.1.4 P7 – Įdarbinimo ir darbo santykių nutraukimo politika: užtikrina kontrolės priemonių priskyrimo ir atšaukimo procesus per personalo gyvavimo ciklo pokyčius.

10.1.5 P33 – Audito ir atitikties stebėsenos politika: remia nepriklausomą valdysenos veiksmingumo peržiūrą ir užtikrina korekcinius veiksmus neatitikties atvejais.

10.2 Šios politikos kartu palaiko vientisą ir privalomai taikomą ISVS valdysenos sistemą.

11. Pamatiniai standartai ir sistemos

11.1 Ši politika yra suderinta su tarptautiniu mastu pripažintais informacijos saugumo valdysenos ir vaidmenų atskaitomybės standartais bei sistemomis. Ji užtikrina atsekamumą iki reglamentavimo ir sertifikavimo reikalavimų bei palaiko dokumentuotais įrodymais grindžiamą ISVS struktūrą.

11.2 ISO/IEC 27001

11.2.1 5.3 punktas – Organizaciniai vaidmenys, atsakomybės ir įgaliojimai: ši politika įgyvendina reikalavimą, kad su informacijos saugumu susiję vaidmenys būtų aiškiai priskirti, perduoti ir dokumentuoti.

11.2.2 9.3 punktas – Vadovybės peržiūra: ši politika užtikrina vykdomąją ISVS vaidmenų ir valdysenos priežiūrą per ketvirtines ir metines peržiūras.

11.2.3 A priedo kontrolė 5.2 – Informacijos saugumo vaidmenys ir atsakomybės: apibrėžia vaidmenis techniniame, operaciniame ir strateginiame lygmenyse, siekiant užtikrinti pareigų atskyrimą (SoD), rizikos savininkystę ir atsekamą atskaitomybę.

11.3 ISO/IEC 27002:2022 – Kontrolė 5

11.3.1 Pateikia įgyvendinimo gaires informacijos saugumo atsakomybių priskyrimui visoje organizacijoje. Ši politika perima šias gaires, apibrėždama vaidmenų tipus, delegavimo taisykles, eskalavimo procedūras ir peržiūros mechanizmus.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1–PL-4: nustato formalaus planavimo dokumentavimo būtinybę, įskaitant politikas, kurios apibrėžia valdyseną ir priskiria su sauga susijusias atsakomybes.

11.4.2 PM-1 (Informacijos saugumo programos planas) ir PM-2 (Vyresnysis informacijos saugumo pareigūnas): šioje politikoje tai atsispindi per vyriausiojo informacijos saugumo pareigūno / ISVS vadovo paskyrimą ir formalius valdysenos vaidmenis.

11.4.3 PM-5–PM-13: ši politika atitinka vaidmenų dokumentavimo, visos organizacijos masto rizikos vaidmenų, konfigūracijos valdymo priežiūros ir integracijos su misijos / verslo funkcijomis reikalavimus.

11.5 ES BDAR (2016/679)

11.5.1 5 straipsnio 1 dalies f punktas: reikalauja apsaugoti asmens duomenis nuo neautorizuoto arba neteisėto tvarkymo. Ši politika užtikrina, kad už duomenų apsaugą atsakingi asmenys būtų aiškiai paskirti ir prižiūrimi.

11.5.2 24 straipsnis: reikalauja tinkamų organizacinių priemonių, įskaitant valdysenos struktūras.

11.5.3 37 straipsnis: reikalauja paskirti duomenų apsaugos pareigūną (DAP), o tai turi būti atspindėta organizacijos valdysenos sistemoje ir atsakomybių registre.

11.6 ES NIS2 direktyva (2022/2555)

11.6.1 21 straipsnio 2 dalies a punktas: nustato, kad subjektai turi įgyvendinti rizikos analizės ir informacinių sistemų saugumo politikas, įskaitant konkretiems vaidmenims priskirtas atsakomybes. Ši politika apibrėžia tokius vaidmenis ir jų valdysenos mechanizmus.

11.7 ES DORA reglamentas (2022/2554)

11.7.1 5 straipsnis – IRT rizikos valdymo ir vidaus kontrolės sistema: reikalauja formaliai priskirti IRT rizikos valdymo atsakomybes, sprendimų priėmimo vaidmenis ir ataskaitų teikimo kanalus. Ši politika sudaro pagrindą su sauga susijusių vaidmenų valdysenai IRT aplinkoje.

11.8 COBIT 2019

11.8.1 EDM01 – Ensured Governance Framework Setting: ši politika užtikrina, kad ISVS turėtų aiškiai apibrėžtą valdysenos struktūrą, suderintą su organizacijos poreikiais.

11.8.2 EDM02 – Ensured Benefits Delivery: suderina vaidmenimis grindžiamas saugumo veiklas su strateginiais ir operaciniais tikslais, užtikrindama atskaitomybę ir išmatuojamus rezultatus.

11.8.3 APO01 – Managed I&T Management Framework ir APO12 – Managed Risk: ši politika palaiko struktūruotą informacijos saugumo vaidmenų valdymą platesnėje IT valdysenos ir rizikos sistemoje.

11.8.4 MEA01 – Monitor, Evaluate and Assess Performance: įtvirtina peržiūros mechanizmus, skirtus patikrinti, kad valdysenos vaidmenys būtų veiksmingi, aktualūs ir taikomi.