					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P02S					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 taikomais standartais ir reglamentais

Standartas / reglamentas	Skyrius / straipsnis	Pastaba
ISO/IEC 27001:2022	5 skyrius	
ISO/IEC 27002:2022	Kontrolės priemonės: 5.2, 5.3, 5.4	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
ES BDAR	5 straipsnio 2 dalis, 32 straipsnis	

1. Tikslas

1.1 Ši politika nustato, kaip organizacijoje priskiriamos, deleguojamos ir valdomos informacijos saugumo valdysenos atsakomybės, siekiant užtikrinti visišką atitiktį ISO/IEC 27001:2022 ir kitiems taikomiems reguliavimo reikalavimams.

1.2 Ji užtikrina atskaitomybę visuose lygmenyse ir padeda palaikyti veiklos efektyvumą, aiškiai nustatydama, kas yra atsakingas už kiekvieną su saugumu susijusią funkciją.

1.3 Ši politika stiprina pasirengimą auditui ir didina klientų pasitikėjimą, įtvirtindama formalią saugumo valdyseną, įskaitant organizacijas, turinčias ribotus techninius išteklius arba besinaudojančias išorės IT paslaugomis.

2. Taikymo sritis

2.1 Ši politika taikoma visiems asmenims, kurie valdo organizacijos sistemas ar duomenis, įskaitant:

2.1.1 verslo savininkus ir generalinį vadovą;

2.1.2 darbuotojus ir rangovus;

2.1.3 išorės IT paslaugų teikėjus ar konsultantus.

2.2 Ji apima visas sistemas, aplinkas ir paslaugas, naudojamas verslo ar klientų informacijai tvarkyti, perduoti ar saugoti, įskaitant:

2.2.1 biuro IT infrastruktūrą ir nuotolinio darbo įrenginius;

2.2.2 debesijos platformas ir el. pašto paslaugas;

2.2.3 fizinius įrašus ir bendruosius diskus.

2.3 Taikymo sritis apima tiek vidaus, tiek išorės paslaugų teikėjams pavestas veiklas, susijusias su informacijos saugumo valdysena.

3. Tikslai

3.1 Nustatyti aiškią atskaitomybę už visas su saugumu susijusias pareigas, įskaitant politikų valdymą, prieigos kontrolę, incidentų valdymą ir stebėseną.

3.2 Užtikrinti veiksmingą pareigų atskyrimą, siekiant sumažinti interesų konfliktų ar sukčiavimo riziką.

3.3 Užtikrinti, kad saugumo užduotys ir vaidmenys būtų aiškiai dokumentuoti ir reguliariai peržiūrimi.

3.4 Sudaryti sąlygas pagrįstam sprendimų priėmimui, eskalavimui ir IT bei saugumo rizikų priežiūrai.

3.5 Palaikyti ISO/IEC 27001:2022 sertifikavimą ir stiprinti klientų, partnerių bei auditorių pasitikėjimą.

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas / verslo savininkas

4.1.1 Atsako už visapusišką šios politikos įgyvendinimą ir priežiūrą.

4.1.2 Tvirtina visus saugumo vaidmenis, atsakomybes ir delegavimo sprendimus.

4.1.3 Vykdo atitikties stebėseną ir priima galutinius sprendimus dėl politikos išimčių bei eskalavimo atvejų.

4.2 Paskirtasis saugumo koordinatorius (jei paskirtas)

4.2.1 Šį vaidmenį gali atlikti darbuotojas arba patikimas konsultantas.

4.2.2 Labai mažose organizacijose šį vaidmenį gali atlikti generalinis vadovas arba išorės paslaugų teikėjas.

4.2.3 Padeda kasdien užtikrinti prieigos kontrolės taikymą, reagavimą į incidentus ir vykdyti bazines technines saugumo užduotis.

4.2.4 Tiesiogiai informuoja generalinį vadovą apie bet kokius saugumo klausimus ar rizikas.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Kasmetinė peržiūra

9.1.1 Šią politiką generalinis vadovas turi peržiūrėti kas 12 mėnesių, siekdamas užtikrinti, kad ji ir toliau atitiktų teisinius įsipareigojimus, veiklos poreikius ir ISO/IEC 27001 sertifikavimo reikalavimus.

9.2 Tarpinės peržiūros

9.2.1 Peržiūros taip pat turi būti atliekamos, kai:

9.2.1.1 įvyksta reikšmingi organizaciniai pokyčiai;

9.2.1.2 pradedamas bendradarbiavimas su nauju paslaugų teikėju;

9.2.1.3 įvyksta rimtas saugumo incidentas;

9.2.1.4 atnaujinami tokie reglamentai kaip ES BDAR, NIS2 direktyva ar DORA reglamentas.

9.3 Versijų valdymas ir dokumentavimas

9.3.1 Visos peržiūros turi apimti:

9.3.1.1 peržiūros datą;

9.3.1.2 visų pakeitimų santrauką;

9.3.1.3 generalinio vadovo parašą arba dokumentuotą patvirtinimą;

9.3.1.4 ankstesnių versijų archyvavimą audito reikmėms.

9.4 Pakeitimų komunikavimas

9.4.1 Visi politikos atnaujinimai turi būti nedelsiant pranešami darbuotojams ir paslaugų teikėjams el. paštu, vidiniuose portaluose arba oficialiais pranešimais.

10. Susijusios politikos ir sąsajos

10.1 Siekiant visapusiško veiksmingumo, ši politika turi būti įgyvendinama kartu su šiomis MVĮ politikomis:

10.1.1 P4S – Prieigos kontrolės politika: nustato, kaip prieiga suteikiama, valdoma ir panaikinama, tiesiogiai susiejant tai su priskirtais vaidmenimis ir priežiūra.

10.1.2 P8S – Informacijos saugumo sąmoningumo ir mokymų politika: sustiprina su vaidmenimis susijusias atsakomybes ir lūkesčius.

10.1.3 P17S – Duomenų apsaugos ir privatumo politika: nustato teisinius įsipareigojimus pagal ES BDAR, kurie priskiriami šioje valdysenos politikoje apibrėžtiems vaidmenims.

10.1.4 P30S – Reagavimo į incidentus politika: reikalauja apibrėžtų atsakomybių už incidentų pranešimą, eskalavimą ir suvaldymą.

10.2 Kartu šios politikos užtikrina nuoseklų taikymą, vidinę atskaitomybę ir išorinę atitiktį.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 5.3 skyrius – Organizaciniai vaidmenys, atsakomybės ir įgaliojimai: reikalauja, kad vaidmenys būtų aiškiai priskirti ir palaikomi aukščiausiosios vadovybės.

11.2 ISO/IEC 27002

11.2.1 5.2–5.4 kontrolės priemonės: nustato aiškaus informacijos saugumo vaidmenų dokumentavimo, pareigų atskyrimo ir vadovybės priežiūros reikalavimus.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: nustato bendrą informacijos saugumo programą su apibrėžtomis atsakomybėmis.

11.3.2 PL-1–PL-4: reikalauja planavimo kontrolės priemonių, įskaitant politikos nustatymą ir dokumentuotą vaidmenų priskyrimą.

11.3.3 CA-1: reikalauja apibrėžtų vertinimo ir įgaliojimų suteikimo vaidmenų.

11.3.4 AC-1: susieja vaidmenimis grindžiamą prieigos kontrolę su priskirtomis valdysenos atsakomybėmis.

11.4 ES BDAR

11.4.1 5 straipsnio 2 dalis – Atskaitomybė: reikalauja, kad organizacijos galėtų pagrįsti atitiktį per vaidmenis ir atsakomybes.

11.4.2 32 straipsnis – Tvarkymo saugumas: pabrėžia aiškų pareigų priskyrimą siekiant apsaugoti asmens duomenis.

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies a punktas: reikalauja valdysenos struktūrų, kuriose būtų formalizuoti vaidmenys kibernetinės rizikos ir incidentų valdymui.

11.6 DORA reglamentas

11.6.1 9 ir 10 straipsniai: reikalauja, kad finansų subjektai aiškiai priskirtų ir prižiūrėtų su IRT ir saugumu susijusias atsakomybes.

11.7 COBIT 2019

11.7.1 EDM03 – Rizikos optimizavimo užtikrinimas: reikalauja aiškiai apibrėžtų vaidmenų ir eskalavimo kelių saugumo rizikai valdyti.

11.7.2 APO13 – Saugumo valdymas: priskiria strategines ir operacines saugumo pareigas asmenims ir vaidmenims.

11.7.3 DSS05 – Saugumo paslaugų valdymas: reikalauja struktūros ir atsekamumo atsakomybėse už išorės ir vidaus saugumo paslaugas.