					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P01S					Dokumento pavadinimas: **Informacijos 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 reglamentais

Standartas / reglamentas	Punktas / straipsnis	Komentaras
ISO/IEC 27001:2022	5.1, 5.2, 5.3, 6.1, 8 punktai	Nustato vadovybės įsipareigojimus, politikos reikalavimus, vaidmenų priskyrimą, rizikos vertinimą ir operacinių kontrolės priemonių valdymą
ISO/IEC 27002:2022	5.1–5 kontrolės priemonės	Nustato dokumentuotų informacijos saugumo politikų rengimo, vaidmenų priskyrimo, pareigų atskyrimo ir vadovybės atsakomybės reikalavimus
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Nustato saugumo programos plano, planavimo politikos, vertinimo ir autorizavimo bei prieigos kontrolės reikalavimus
ES BDAR (2016/679)	5 straipsnio 2 dalis, 32 straipsnis	Nustato atskaitomybės principą ir duomenų tvarkymo saugumo priemones, ypač susijusias su dokumentuotais vaidmenimis
ES NIS2 direktyva (2022/2555)	21 straipsnio 2 dalies a punktas	Reikalauja kibernetinių rizikų valdymo priemonių, vaidmenų ir atsakomybių
ES DORA reglamentas (2022/2554)	9 straipsnis, 10 straipsnis	Reikalauja priskirti vaidmenis IRT rizikos valdymui ir veiklos tęstinumui
COBIT 2019	EDM03, APO13, DSS05	Užtikrina rizikos optimizavimą, saugumo valdymą ir saugumo paslaugų valdymą, aiškiai priskiriant vaidmenis

1. Tikslas

1.1 Ši politika patvirtina organizacijos įsipareigojimą saugoti klientų ir verslo informaciją, aiškiai nustatant atsakomybes ir praktines saugumo priemones, tinkamas organizacijoms, neturinčioms specializuotų IT komandų.

1.2 Ji užtikrina, kad visi darbuotojai, rangovai ir paslaugų teikėjai laikytųsi privalomų taisyklių, sudarančių prielaidas visiškai atitikti ISO/IEC 27001 sertifikavimo reikalavimus.

1.3 Ši politika padeda organizacijai stiprinti klientų pasitikėjimą, aiškiai parodant, kaip jų informacija saugoma pasitelkiant apibrėžtas atsakomybes, struktūruotus procesus ir aiškią atskaitomybę.

2. Taikymo sritis

2.1 Ši politika taikoma visiems asmenims, kurie turi prieigą prie organizacijos duomenų ir sistemų arba juos valdo, įskaitant:

2.1.1 Verslo savininkus ir generalinius vadovus

2.1.2 Darbuotojus, rangovus ir praktikantus

2.1.3 Išorės IT paslaugų teikėjus arba konsultantus

2.2 Ji apima visų rūšių informaciją, sistemas ir paslaugas, įskaitant:

2.2.1 Veiklos įrašus, klientų duomenis, slaptažodžius ir elektroninius laiškus

2.2.2 IT įrangą, pavyzdžiui, nešiojamuosius kompiuterius ir telefonus

2.2.3 Debesijos paslaugas, naudojamas failams saugoti, komunikacijai ar finansų valdymui

2.2.4 Fizinius dokumentus, saugomus biuro patalpose

2.3 Politika taikoma visose darbo aplinkose – biure, dirbant nuotoliniu būdu ir debesijos aplinkoje – ir apima visus įrenginius bei programinę įrangą, naudojamus verslo informacijai tvarkyti ar saugoti.

3. Tikslai

3.1 Aiškiai priskirti atsakomybę: užtikrinti, kad už informacijos saugumą visada būtų paskirtas atsakingas asmuo. Paprastai tai yra generalinis vadovas arba jo oficialiai paskirtas asmuo.

3.2 Saugoti klientų ir verslo informaciją: taikyti patikimas ir nuoseklias apsaugos priemones, kad būtų išvengta netinkamo naudojimo, praradimo ar vagystės, įskaitant klientų ir finansinius įrašus.

3.3 Remti ISO/IEC 27001 sertifikavimą: sudaryti organizacijai sąlygas įrodyti visišką atitiktį ISO/IEC 27001 reikalavimams, užtikrinti pasirengimą auditui ir tinkamumą sertifikavimui, nereikalaujant sudėtingos infrastruktūros.

3.4 Integruoti saugumą į veiklą: integruoti informacijos saugumą į kasdienes užduotis ir sprendimų priėmimą visoje organizacijoje.

3.5 Stiprinti saugumo suvokimą ir kultūrą: skatinti kiekvieną darbuotoją suprasti ir laikytis saugumo praktikos, pavyzdžiui, naudoti stiprius slaptažodžius ir pranešti apie įtartiną veiklą.

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas arba verslo savininkas

4.1.1 Prisiima visą atsakomybę už informacijos saugumą.

4.1.2 Tvirtina ir prižiūri šią politiką.

4.1.3 Užtikrina, kad visos pagrindinės saugumo užduotys būtų vykdomos tiesiogiai arba deleguotos raštu.

4.1.4 Tikrina, kad visos deleguotos saugumo užduotys, pavyzdžiui, prieigos valdymas ar reagavimas į incidentus, būtų vykdomos veiksmingai.

4.1.5 Veikia kaip pagrindinis kontaktinis asmuo visais vidaus ir išorės saugumo klausimais, įskaitant auditus ir klientų užklausas.

4.1.6 Kasmetinės peržiūros metu stebi pažangą pagal šiuos tikslus. Jei įmanoma, tikslai turi būti išmatuojami (pvz., apmokytų darbuotojų procentas, užregistruotų incidentų skaičius ir pan.) ir peržiūrimi atsižvelgiant į saugumo incidentus bei rizikos pokyčius.

4.2 Paskirtas darbuotojas (jei taikoma)

4.2.1 Gali padėti generaliniam vadovui vykdydamas kasdienes užduotis, pavyzdžiui, kurdamas naudotojų paskyras, panaikindamas prieigą išėjusiems darbuotojams arba koordinuodamas veiksmus su IT paslaugų teikėju.

4.2.2 Turi būti oficialiai paskirtas ir turėti pakankamus įgaliojimus bei išteklius užduotims vykdyti.

4.2.3 Apie visas problemas praneša generaliniam vadovui.

[... 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 (GV) privalo peržiūrėti bent kartą per metus, kad būtų užtikrinta nuolatinė atitiktis ISO/IEC 27001 sertifikavimo reikalavimams, reguliavimo pokyčiams (pvz., ES BDAR, NIS2 direktyvai ir DORA reglamentui) bei kintantiems verslo poreikiams.

9.2 Tarpinės peržiūros

9.2.1 Papildomos peržiūros turi būti atliekamos kiekvieną kartą, kai įvyksta reikšmingų pokyčių, pavyzdžiui:

9.2.1.1 Dideli saugumo incidentai ar pažeidimai.

9.2.1.2 Naujų verslo procesų ar technologijų įdiegimas (pvz., nauja programinė įranga, nuotolinio darbo platformos ar debesijos paslaugos).

9.2.1.3 Teisinių ar reguliavimo reikalavimų, turinčių įtakos informacijos tvarkymui, pasikeitimai.

9.3 Pakeitimų dokumentavimas

9.3.1 Visos politikos peržiūros ir pakeitimai turi būti oficialiai dokumentuojami, aiškiai nurodant datą, pakeitimų pobūdį ir GV patvirtinimą.

9.3.2 Istorinis politikos versijų įrašas turi būti saugiai tvarkomas, kad audito metu būtų galima parodyti politikos raidą ir atitiktį.

9.4 Atnaujinimų komunikavimas

9.4.1 Bet kokie šios politikos pakeitimai turi būti nedelsiant pranešami visiems darbuotojams, rangovams ir susijusioms trečiosioms šalims.

9.4.2 Atnaujintos politikos versijos turi būti lengvai prieinamos visam paveiktam personalui (pvz., pateikiamos elektroniniu būdu arba fiziškai paskelbiamos darbo vietoje).

10. Susijusios politikos ir sąsajos

10.1 Ši politika glaudžiai susijusi su kitomis organizacijos SME politikų rinkinio politikomis, visų pirma:

10.1.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: paaiškina saugumo pareigų ir atsakomybių priskyrimą.

10.1.2 P4S – Prieigos kontrolės politika: apibrėžia saugų prieigos prie organizacijos informacijos valdymą.

10.1.3 P8S – Informacijos saugumo suvokimo ir mokymų politika: nustato pagrindines darbuotojų mokymų ir saugumo suvokimo gaires.

10.1.4 P17S – Duomenų apsaugos ir privatumo politika: užtikrina atitiktį ES BDAR ir kitiems duomenų apsaugos teisės aktams.

10.1.5 P30S – Reagavimo į incidentus politika: aprašo išsamius veiksmus, kurių reikia imtis reaguojant į saugumo incidentus.

10.2 Šios susijusios politikos nustato aiškias operacines gaires ir turi būti įgyvendinamos kartu, siekiant visiškos atitikties ISO/IEC 27001 sertifikavimo reikalavimams.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 5.1 punktas – Lyderystė ir įsipareigojimas: reikalauja aukščiausios vadovybės įsipareigojimo ir atsakomybės už informacijos saugumo veiksmingumą organizacijoje.

11.1.2 5.2 punktas – Informacijos saugumo politika: nustato aiškių, dokumentuotų politikų, suderintų su organizacijos strategija ir atitikties reikalavimais, būtinybę.

11.1.3 5.3 punktas – Organizaciniai vaidmenys ir atsakomybės: apibrėžia aiškų informacijos saugumo atsakomybių priskyrimą visoje organizacijoje, kuris būtinas veiksmingai valdysenai ir atitikčiai audito reikalavimams.

11.1.4 6.1 punktas – Veiksmai rizikoms ir galimybėms valdyti: užtikrina, kad informacijos saugumo rizikos būtų sistemiškai nustatomos, vertinamos ir tvarkomos.

11.1.5 8.1 punktas – Operacinis planavimas ir kontrolė: reikalauja organizacijai planuoti ir įgyvendinti procesus, reikalingus informacijos saugumo tikslams pasiekti ir susijusioms rizikoms veiksmingai valdyti.

11.2 ISO/IEC 27002:2022 5.1–5 kontrolės priemonės

11.2.1 A priedo 5.1 kontrolės priemonė – Informacijos saugumo politikos: nustato dokumentuotų informacijos saugumo politikų rengimo ir komunikavimo reikalavimus.

11.2.2 A priedo 5.2 kontrolės priemonė – Informacijos saugumo vaidmenys: paaiškina ir oficialiai priskiria informacijos saugumo vaidmenis bei atsakomybes susijusioms šalims.

11.2.3 A priedo 5.3 kontrolės priemonė – Pareigų atskyrimas: nustato aiškų pareigų atskyrimą siekiant sumažinti interesų konfliktų ir sukčiavimo riziką tvarkant jautrią informaciją.

11.2.4 A priedo 5.4 kontrolės priemonė – Vadovybės atsakomybės: reikalauja, kad vadovybė rodytų įsipareigojimą informacijos saugumui aktyvia priežiūra ir išteklių skyrimu.

11.2.5 Sustiprina aiškiai dokumentuotų informacijos saugumo politikų, vaidmenų, atsakomybių ir valdysenos struktūrų būtinybę, užtikrinant nuoseklų valdymą ir audito atsekamumą visoje organizacijoje.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Informacijos saugumo programos planas: reikalauja dokumentuotų informacijos saugumo valdysenos strategijų ir politikų, sudarančių pagrindą nuosekliam įgyvendinimui ir valdymui.

11.3.2 PL-1 – Saugumo planavimo politika: nustato visos organizacijos mastu taikomą saugumo planavimo politiką, kuri turi užtikrinti saugų veikimą ir strateginį informacijos saugumo veiklų suderinimą.

11.3.3 CA-1 – Saugumo vertinimo ir autorizavimo politika: reikalauja aiškiai apibrėžtų vertinimo ir autorizavimo vaidmenų, kad būtų užtikrintas nuolatinis veiksmingumas ir atitiktis informacijos saugumo reikalavimams.

11.3.4 AC-1 – Prieigos kontrolės politika: reikalauja, kad organizacijos aiškiai apibrėžtų, dokumentuotų ir įgyvendintų prieigos valdymo praktiką bei atsakomybes.

11.4 ES BDAR (2016/679)

11.4.1 5 straipsnio 2 dalis – Atskaitomybės principas: reikalauja, kad organizacijos galėtų įrodyti atitiktį duomenų apsaugos principams, įskaitant dokumentuotus vaidmenis ir politikas, susijusias su duomenų apsaugos atsakomybėmis.

11.4.2 32 straipsnis – Duomenų tvarkymo saugumas: nustato pareigą įgyvendinti tinkamas technines ir organizacines priemones, įskaitant aiškias saugumo atsakomybes, siekiant apsaugoti asmens duomenis nuo pažeidimų ir neautorizuotos prieigos.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21 straipsnio 2 dalies a punktas – Rizikos valdymo priemonės: reikalauja aiškios valdysenos tvarkos, įskaitant apibrėžtus informacijos saugumo vaidmenis ir atsakomybes, kurios būtinos veiksmingam kibernetinių rizikų valdymui.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 9 straipsnis – IRT rizikos valdymas: reikalauja, kad organizacijos aiškiai priskirtų vaidmenis ir atsakomybes, susijusias su IRT rizikos valdymu, taip stiprinant atsparumą ir pasirengimą veiklos tęstinumui.

11.6.2 10 straipsnis – IRT veiklos tęstinumas: reikalauja aiškios atskaitomybės ir struktūruotų vaidmenų IRT atsparumui ir veiklos tęstinumui palaikyti, užtikrinant, kad organizacijos galėtų patikimai reaguoti į sutrikimus.

11.7 COBIT 2019

11.7.1 EDM03 – Užtikrinti rizikos optimizavimą: pabrėžia aiškiai apibrėžtą atskaitomybę ir vaidmenis valdant organizacijos rizikas, užtikrinant tvirtą valdyseną ir veiksmingą informacijos saugumo rizikų priežiūrą.

11.7.2 APO13 – Valdyti saugumą: reikalauja, kad organizacijos aiškiai nustatytų ir komunikuotų saugumo valdymo atsakomybes, užtikrindamos suderinamumą su verslo tikslais ir reguliavimo reikalavimais.

11.7.3 DSS05 – Valdyti saugumo paslaugas: numato struktūruotus vaidmenis ir aiškias atsakomybes valdant saugumo paslaugas, kad būtų užtikrintas nuoseklus įgyvendinimas ir atitikties tikrinimas.