					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P01					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**

Teisinis pranešimas (autorių teisės ir naudojimo apribojimai)

(C) 2025 Clarysec LLC. All rights reserved.

Šis dokumentas yra Clarysec LLC intelektinė nuosavybė. Jokia šio dokumento dalis negali būti kopijuojama, pakartotinai naudojama, platinama ar keičiama komerciniais ar įgyvendinimo tikslais be išankstinio aiškaus rašytinio leidimo.

Neautorizuotas naudojimas yra griežtai draudžiamas ir gali užtraukti teisinius veiksmus.

Dėl licencijavimo kreipkitės: info@clarysec.com

1. Tikslas

1.1 Ši politika nustato bendrą organizacijos įsipareigojimą užtikrinti informacijos saugumą, įdiegiant formalizuotą informacijos saugumo valdymo sistemą (ISVS).

1.2 Ji nustato strateginę kryptį ir pagrindinius reikalavimus, skirtus visų informacijos išteklių konfidencialumui, vientisumui, prieinamumui ir atsparumui užtikrinti fizinėse, skaitmeninėse ir debesijos aplinkose.

1.3 Ši politika įgyvendina ISO/IEC 27001:2022 5.1 ir 5.2 skyrių reikalavimus, nes išreiškia vadovybės ketinimus, aukščiausiosios vadovybės įsipareigojimą ir saugumo veiklų suderinimą su organizacijos tikslais.

1.4 Ji yra pagrindinis atskaitos dokumentas visoms pavaldžiosioms ISVS politikoms, standartams ir procedūroms ir yra būtina siekiant užtikrinti rizika grindžiamą, į atitiktį orientuotą ir nuolat tobulinamą saugumo aplinką.

2. Taikymo sritis

2.1 Ši politika taikoma visiems asmenims, ištekliams ir procesams, apibrėžtiems ISVS taikymo srityje, įskaitant:

2.1.1 visus verslo padalinius, skyrius, patronuojamąsias bendroves ir filialus

2.1.2 darbuotojus, rangovus, laikinąjį personalą, konsultantus ir trečiųjų šalių paslaugų teikėjus

2.1.3 visus duomenis, informacines sistemas, taikomąsias programas, infrastruktūrą ir ryšių kanalus

2.1.4 visas fizines, debesijos, nuotolines ir hibridines aplinkas, kuriose tvarkomi bendrovės duomenys arba prie jų jungiamasi

2.2 Ši politika yra privaloma visiems subjektams, tvarkantiems organizacijos informaciją, ir taikoma visais informacijos gyvavimo ciklo etapais – nuo sukūrimo ir perdavimo iki saugojimo ir sunaikinimo.

2.3 Bet kokios šios taikymo srities išimtys ar apribojimai turi būti dokumentuoti ISVS taikymo srities apraše ir pagrįsti formaliu vykdomosios vadovybės patvirtinimu.

3. Tikslai

3.1 Sukurti su ISO/IEC 27001:2022 suderintą ISVS, sudarančią sąlygas visos organizacijos mastu priimti rizika grindžiamus sprendimus.

3.2 Užtikrinti, kad konfidencialumo, vientisumo ir prieinamumo principai būtų integruoti į visas organizacijos veiklas, sistemas ir partnerystes.

3.3 Užtikrinti teisės aktų, reguliavimo ir sutarčių reikalavimų laikymąsi, nustatant išmatuojamus, politika grindžiamus saugumo tikslus ir integruojant juos į verslo veiklą.

3.4 Mažinti informacijos saugumo incidentų tikimybę ir poveikį taikant veiksmingas prevencines, aptikimo ir korekcines kontrolės priemones.

3.5 Užtikrinti nuolatinį informacijos saugumo brandos didinimą, remiantis nustatytais veiklos rodikliais, audito rezultatais ir vadovybės peržiūromis.

3.6 Stiprinti atskaitomybės, sąmoningumo ir atsparumo kultūrą, kurioje kiekvienam darbuotojui saugumo atsakomybės yra aiškiai apibrėžtos ir vykdomos.

4. Vaidmenys ir atsakomybės

4.1 Vykdomoji vadovybė

4.1.1 Tvirtina Informacijos saugumo politiką ir ISVS.

4.1.2 Užtikrina saugumo tikslų suderinimą su verslo strategija.

4.1.3 Rodo asmeninį pavyzdį ir stiprina informacijos saugumo kultūrą.

4.1.4 Peržiūri ir tvirtina esminius ISVS taikymo srities, rizikos tvarkymo ir valdysenos struktūros pakeitimus.

4.2 Informacijos saugumo vadovas (CISO) / ISVS vadovas

4.2.1 Atsako už ISVS ir užtikrina, kad ši politika būtų palaikoma laikantis ISO/IEC 27001 reikalavimų.

4.2.2 Vadovauja rizikos vertinimo, kontrolės priemonių įgyvendinimo ir nuolatinio tobulinimo procesams.

4.2.3 Užtikrina tarpfunkcinį saugumo veiklų koordinavimą ir prižiūri pavaldžiąsias politikas.

4.2.4 Teikia vykdomajai vadovybei informaciją apie ISVS būklę, incidentus, audito rezultatus ir rodiklius.

4.2.5 Užtikrina, kad politikos peržiūros ir atnaujinimai būtų atliekami pagal šio dokumento 9 skyrių.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Peržiūros periodiškumas

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

9.1.1.1 esminiams teisinių, reguliavimo ar sutartinių įsipareigojimų pokyčiams

9.1.1.2 esminiams organizacijos rizikos profilio pokyčiams

9.1.1.3 vidaus ar išorės auditų rezultatams

9.1.1.4 reikšmingiems incidentams ar kontrolės priemonių veikimo sutrikimams

9.2 Peržiūros atsakomybė ir procesas

9.2.1 CISO arba paskirtas ISVS vadovas vadovauja peržiūros procesui.

9.2.2 Peržiūros įvestis turi apimti:

9.2.2.1 vidaus audito rezultatus

9.2.2.2 rizikos vertinimo tendencijas

9.2.2.3 verslo procesų ir technologijų pokyčius

9.2.2.4 KPI rezultatus ir rizikos slenksčių laikymąsi

9.2.3 Visi atnaujinimai turi:

9.2.3.1 būti valdomi versijomis ir dokumentuojami

9.2.3.2 būti patvirtinti vykdomosios vadovybės

9.2.3.3 būti pateikti visoms susijusioms šalims oficialiais komunikacijos kanalais

9.2.3.4 lemti reikalingus pavaldžiosios dokumentacijos ir mokymų atnaujinimus

10. Susijusios politikos ir sąsajos

10.1 Ši pagrindinė politika yra tiesiogiai susieta su šiomis organizacijos saugumo politikomis ir sistemomis:

10.1.1 P2 – Valdysenos vaidmenų ir atsakomybių politika: nustato šiame dokumente nurodytą valdysenos struktūrą ir įgaliojimų hierarchiją.

10.1.2 P3 – Priimtino naudojimo politika: nustato elgesio reikalavimus ir tinkamą informacijos išteklių naudojimą.

10.1.3 P4 – Prieigos kontrolės politika: detalizuoja iš šios pagrindinės politikos išvestas su prieiga susijusias kontrolės priemones.

10.1.4 P6 – Rizikos valdymo politika: nustato rizika grindžiamą kontekstą kontrolės priemonių parinkimui ir liekamosios rizikos priėmimui.

10.1.5 P33 – Audito ir atitikties stebėsenos politika: nustato, kaip vidaus užtikrinimo mechanizmai patvirtina politikos taikymą.

10.2 Šios tarpusavio sąsajos užtikrina visapusišką suderinamumą ir atsekamumą visoje ISVS bei palaiko vieningą rizikos ir atitikties valdyseną.

11. Pamatiniai standartai ir sistemos

11.1 Ši Informacijos saugumo politika yra formaliai suderinta su toliau nurodytais standartais ir sistemomis, siekiant užtikrinti visišką atitiktį, pasirengimą auditui ir galimybę pagrįsti atitiktį reguliavimo reikalavimams:

11.2 ISO/IEC 27001

11.2.1 5.1 skyrius – Lyderystė ir įsipareigojimas: ši politika parodo aukščiausiosios vadovybės įsipareigojimą informacijos saugumui ir nustato ISVS atsakomybes bei išteklių paskirstymą.

11.2.2 5.2 skyrius – Informacijos saugumo politika: šis dokumentas yra oficiali organizacijos saugumo politika, suderinta su nustatytais saugumo tikslais, verslo strategija ir ISO/IEC 27001 atitikties reikalavimais.

11.2.3 6.1 skyrius – Veiksmai rizikoms ir galimybėms valdyti: šioje politikoje įtvirtintas rizika grindžiamas požiūris užtikrina, kad saugumo ištekliai būtų taikomi proporcingai grėsmėms.

11.2.4 9.2 skyrius – Vidaus auditas ir 10 skyrius – Tobulinimas: ši politika yra integruota į organizacijos nuolatinio tobulinimo ciklą ir jai taikomas vidaus audito patvirtinimas.

11.2.5 ISO/IEC 27002:2022 – 5.1 kontrolė: pateikia gaires saugumo politikoms nustatyti ir palaikyti. Ši politika atitinka ISO 27002 rekomendacijas dėl hierarchinės dokumentacijos, peržiūros ciklų ir taikymo.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (saugumo planavimo politika ir procedūros): ši politika atitinka reikalavimą parengti, paskelbti ir peržiūrėti formalią visos organizacijos informacijos saugumo politiką.

11.3.2 PM-1 iki PM-5: apima programos lygmens valdyseną, įskaitant informacijos saugumo vaidmenis, išteklių paskirstymą, rizikos strategiją ir saugumo planavimo integravimą į organizacijos veiklą.

11.4 ES BDAR (2016/679)

11.4.1 5 straipsnio 2 dalis: įtvirtina atskaitomybės principą. Ši politika nustato atsakingas šalis ir atsekamus taikymo veiksmus.

11.4.2 24 straipsnis: reikalauja įgyvendinti technines ir organizacines priemones, įskaitant rizika grindžiamas politikas.

11.4.3 32 straipsnis: palaiko tinkamų priemonių įgyvendinimą asmens duomenų saugumui užtikrinti per visą jų gyvavimo ciklą.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21 straipsnio 2 dalies a punktas: įpareigoja subjektus įgyvendinti dokumentuotą saugumo politiką, apimančią rizikos valdymą ir valdyseną. Ši politika atitinka šį reikalavimą ir palaiko platesnį kibernetinio saugumo pasirengimą bei ypatingos svarbos infrastruktūros apsaugą.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 5 straipsnio 2 dalis: reikalauja dokumentuotos vidaus kontrolės sistemos IRT rizikai valdyti. Ši politika palaiko finansų sektoriaus atitiktį, nustatydama vaidmenis, kontrolės priemones ir priežiūros funkcijas pagal DORA valdysenos lūkesčius.

11.7 COBIT 2019

11.7.1 EDM01 – Valdysenos sistemos nustatymas: ši politika palaiko organizacijos valdyseną, nustatydama ISVS vaidmenis, vadovybės įsipareigojimus ir strateginius tikslus.

11.7.2 APO01 – Valdymo sistema: palaiko struktūruotos ISVS sukūrimą ir veikimą.

11.7.3 APO12 – Rizikos valdymas: suteikia pagrindą informacijos saugumo rizikos valdysenai.

11.7.4 MEA01/MEA03 – Stebėti, vertinti ir įvertinti: stiprina nuolatinį veiklos vertinimą ir vidaus kontrolės stebėseną užtikrinant politikos laikymąsi.