					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P37S					Dokumento pavadinimas: **Teisinės ir reguliacinės atitikties 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	Skyrius / straipsnis	Komentaras
ISO/IEC 27001:2022	5.1, 6.1, 6.2, 8 skyriai	
ISO/IEC 27002:2022	Kontrolė 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
ES BDAR	5, 6, 32, 33 straipsniai	
ES TIS2 direktyva	21(2)(a), 21(2)(f), 23 straipsniai	
ES DORA reglamentas	5(2), 9(1), 17 straipsniai	
COBIT 2019	APO12, APO13, DSS01	

1. Tikslas

1.1 Ši politika apibrėžia organizacijos požiūrį į teisinių, reguliacinių ir sutartinių įsipareigojimų nustatymą, jų laikymąsi ir gebėjimą pagrįsti atitiktį.

1.2 Ji nustato aiškias atsakomybes ir praktinius veiksmus, padedančius organizacijai vykdyti atitikties pareigas, įskaitant duomenų apsaugos teisės aktus, kibernetinio saugumo sistemas, klientų sutartis ir sertifikavimo standartus.

1.3 Ji užtikrina, kad net ir neturėdama specializuotos atitikties komandos, organizacija galėtų palaikyti teisiškai pagrįstą veiklą, tinkamai reaguoti į incidentus ir išlaikyti pasirengimą auditui.

1.4 Ši politika yra būtina siekiant ISO/IEC 27001:2022 sertifikavimo ir tenkinant išorinių klientų, reguliuotojų ar partnerių lūkesčius.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 visiems darbuotojams, rangovams, laisvai samdomiems specialistams ir trečiųjų šalių tiekėjams;

2.1.2 visoms paslaugoms, operacijoms, sistemoms ir duomenų tvarkymo veikloms, kai organizacija privalo laikytis teisinių ar sutartinių reikalavimų;

2.1.3 visoms vietoms ir įrenginiams, naudojamiems veiklos informacijai tvarkyti, nepriklausomai nuo to, ar jie yra biure, nuotolinėje darbo vietoje, ar debesijos sistemose.

2.2 Politika apima:

2.2.1 duomenų apsaugos teisės aktus, tokius kaip ES BDAR;

2.2.2 kibernetinio saugumo reglamentavimą, tokį kaip ES TIS2 direktyva;

2.2.3 sektoriui taikomus įpareigojimus, kai taikoma;

2.2.4 klientų sutartis, konfidencialumo susitarimus ir audito nuostatas;

2.2.5 savanorišką sertifikavimą (pvz., ISO 27001) ir vidaus politikas, kurių laikymasis būtinas atitikties užtikrinimui.

3. Tikslai

3.1 Nustatyti atskaitomybę: aiškiai priskirti atsakomybę už teisinių, reguliacinių ir sutartinių įsipareigojimų stebėseną, atnaujinimą ir taikymą.

3.2 Apsaugoti organizaciją: mažinti teisės pažeidimų, baudų, duomenų saugumo pažeidimų ir reputacinės žalos riziką.

3.3 Užtikrinti pasirengimą auditui: palaikyti patikrinamus įrašus, rodančius, kaip organizacija vykdo savo atitikties įsipareigojimus.

3.4 Užtikrinti politikų integraciją: užtikrinti, kad teisinės ir reguliacinės pareigos būtų nuosekliai taikomos visose politikose ir procesuose.

3.5 Skaidriai valdyti išimtis: užtikrinti, kad visos atitikties išimtys būtų dokumentuotos, pagrįstos ir patvirtintos, siekiant išvengti atsakomybės rizikos.

4. Vaidmenys ir atsakomybės

4.1 Generalinis direktorius (GD)

4.1.1 prisiima bendrą atskaitomybę už organizacijos teisinę ir reguliacinę atitiktį;

4.1.2 tvarko Atitikties registrą ir užtikrina, kad jis būtų nuolat atnaujinamas;

4.1.3 peržiūri klientų sutartis ir užtikrina, kad konkretūs įsipareigojimai būtų stebimi ir taikomi;

4.1.4 tvirtina atitikties įsipareigojimų išimtis tik tais atvejais, kai jos yra teisiškai pagrįstos ir taikomos kompensuojamosios kontrolės priemonės.

4.2 Išorės konsultantai (pvz., teisės, IT ar atitikties konsultantai)

4.2.1 padeda GD nustatyti taikytinus teisės aktus, sertifikavimo reikalavimus ir įsipareigojimus (pvz., ES BDAR, TIS2, ISO 27001);

4.2.2 teikia gaires dėl naujų reglamentų ar galiojančių teisės aktų pakeitimų aiškinimo;

4.2.3 prireikus gali padėti atnaujinti politikas, atlikti auditus ar reaguoti į pažeidimus, kai kyla teisinė rizika.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Planinė metinė peržiūra

9.1.1 Ši politika turi būti peržiūrima kas 12 mėnesių GD.

9.1.2 Peržiūra turi patvirtinti:

9.1.2.1 aktualumą esamam teisiniam ir sutartiniam kontekstui;

9.1.2.2 tinkamą klientų susitarimų ir paslaugų įsipareigojimų atspindėjimą;

9.1.2.3 suderinamumą su Atitikties registru ir kitomis politikomis.

9.2 Įvykiais grindžiami atnaujinimai

9.2.1 Nedelsiama peržiūra privaloma, jei:

9.2.1.1 pradedamas taikyti naujas teisės aktas ar reguliacinis reikalavimas (pvz., nauja duomenų apsaugos taisyklė);

9.2.1.2 klientas į savo sutartį įtraukia sudėtingas atitikties sąlygas;

9.2.1.3 įvyksta pažeidimas ar neatitikties incidentas;

9.2.1.4 bendrovė plečiasi į reguliuojamą rinką ar sektorių.

9.3 Atnaujinimų tvirtinimas ir versijų kontrolė

9.3.1 Visi atnaujinimai turi būti dokumentuojami, valdomi taikant versijų kontrolę ir tvirtinami GD.

9.3.2 Ankstesnės versijos turi būti saugomos audito ir teisiniais tikslais.

9.4 Pranešimas apie pakeitimus

9.4.1 Darbuotojai ir rangovai turi būti informuoti apie politikos pakeitimus per 5 darbo dienas nuo jų patvirtinimo.

9.4.2 Visi paveikti tiekėjai taip pat turi patvirtinti atnaujintas sąlygas prieš toliau teikdami paslaugas.

10. Susijusios politikos ir sąsajos

10.1 Ši politika palaikoma ir įgyvendinama per šias MVĮ politikas:

10.1.1 P3S – Priimtino naudojimo politika: padeda išvengti elgesio, kuris gali pažeisti teisines ar sutartines sąlygas (pvz., nesankcionuoto failų bendrinimo);

10.1.2 P8S – Informacijos saugumo supratimo ir mokymo politika: supažindina darbuotojus su atitikties įsipareigojimais ir tuo, kaip išvengti pažeidimų;

10.1.3 P14S – Duomenų saugojimo ir sunaikinimo politika: užtikrina teisėtą duomenų tvarkymo praktiką per visą duomenų gyvavimo ciklą;

10.1.4 P17S – Duomenų apsaugos ir privatumo politika: užtikrina ES BDAR ir klientų duomenų tvarkymo reikalavimų laikymąsi;

10.1.5 P30S – Reagavimo į incidentus politika: nustato, kaip reaguoti į duomenų saugumo pažeidimus ar atitikties nesėkmes, įskaitant pranešimo terminus;

10.1.6 P36S – Socialinių tinklų ir išorinės komunikacijos politika: užtikrina, kad viešoji komunikacija nepažeistų teisinių ar reguliacinių įsipareigojimų.

10.2 Kiekviena susijusi politika įgyvendina dalį teisinės atitikties sistemos ir turi būti taikoma kartu.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 6.1 skyrius – veiksmai rizikoms ir galimybėms spręsti: apima atitikties rizikas.

11.1.2 8.1 skyrius – veiklos planavimas ir valdymas: reikalauja vykdyti procesus, atitinkančius teisinius ir sutartinius reikalavimus.

11.2 ISO/IEC 27002

11.2.1 Kontrolė 5.36 – pateikia gaires organizacijai dėl įsipareigojimų įrašų tvarkymo ir tinkamo reagavimo į teisinius bei reguliacinius poreikius.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – politika ir procedūros: reikalauja formalių atitikties politikų.

11.3.2 PM-1 – informacijos saugumo programos planas: reikalauja integruoti teisinę atitiktį į saugumo planavimą.

11.3.3 CA-1 – vertinimas, autorizavimas ir stebėsena.

11.3.4 AU-1 – audito politika: reikalauja palaikyti atitikties įrodymus.

11.4 ES BDAR

11.4.1 5 straipsnis – duomenų tvarkymo principai, įskaitant atskaitomybę.

11.4.2 6 straipsnis – teisinis tvarkymo pagrindas.

11.4.3 32 straipsnis – tvarkymo saugumas.

11.4.4 33 straipsnis – pranešimas apie pažeidimą per 72 valandas.

11.5 ES TIS2 direktyva

11.5.1 21(2)(a) ir (f) straipsniai – vidaus politikos rizikos ir reguliacinės kontrolės užtikrinimui.

11.5.2 23 straipsnis – įgyvendinimas ir sankcijos už atitikties nesėkmes.

11.6 ES DORA reglamentas

11.6.1 5(2) straipsnis – IRT rizikos valdymo priežiūra.

11.6.2 9(1) straipsnis – vidaus atitikties valdysena.

11.6.3 17 straipsnis – sutartiniai susitarimai su IRT paslaugų teikėjais.

11.7 COBIT 2019

11.7.1 APO12 – valdoma rizika: užtikrina, kad atitikties rizikos būtų stebimos ir valdomos.

11.7.2 APO13 – valdomas saugumas: apima rizika grindžiamą reguliacinės ir sutartinės atitikties taikymą.

11.7.3 DSS01 – valdomos operacijos: reikalauja veiklos pasirengimo vykdyti teisinius įsipareigojimus.