					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P37					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**

1. Tikslas

1.1 Ši politika nustato privalomą sistemą, skirtą identifikuoti, valdyti ir užtikrinti visų teisinių, reguliacinių ir sutartinių įpareigojimų, susijusių su organizacijos informacijos saugumu, duomenų privatumu ir veiklos funkcijomis, laikymąsi.

1.2 Politikos tikslas – užkirsti kelią neatitikčiai, dėl kurios gali būti skiriamos baudos, kilti teisinė atsakomybė, atsirasti veiklos sutrikimų, reputacinės žalos ar reguliavimo institucijų taikomų poveikio priemonių.

1.3 Ši politika padeda integruoti atitikties reikalavimus į valdyseną, rizikos valdymą, operacinius procesus, projektų gyvavimo ciklus ir sistemų projektavimą.

1.4 Ji užtikrina, kad visi aktualūs įpareigojimai įvairiose jurisdikcijose, pramonės sektoriuose ir reguliavimo srityse būtų aiškiai dokumentuojami, vertinami, stebimi ir įgyvendinami organizacijoje.

2. Taikymo sritis

2.1 Ši politika taikoma visiems departamentams, funkcijoms, verslo padaliniams ir asmenims, veikiantiems organizacijos vardu, įskaitant:

2.1.1 nuolatinius ir laikinus darbuotojus

2.1.2 rangovus, konsultantus ir praktikantus

2.1.3 trečiųjų šalių tiekėjus, duomenų tvarkytojus ar partnerius, tvarkančius organizacijos duomenis, sistemas arba vykdančius su reguliacine atitiktimi susijusias atsakomybes

2.1.4 bet kokį verslo procesą, projektą ar iniciatyvą, kuriems taikoma teisinė ar reguliacinė kontrolė

2.2 Šios politikos reglamentuojamos atitikties sritys apima, bet jomis neapsiribojama:

2.2.1 informacijos saugumo ir kibernetinio saugumo įpareigojimus (pvz., ISO/IEC 27001, NIS2, DORA)

2.2.2 duomenų apsaugos ir privatumo teisės aktus (pvz., BDAR, konkretiems sektoriams taikomus privatumo teisės aktus)

2.2.3 sektorių reguliavimą (pvz., finansų, medicinos, automobilių, gynybos)

2.2.4 sutartinius įpareigojimus, kylančius iš konfidencialumo susitarimų, paslaugų lygio susitarimų (SLA) ar trečiųjų šalių duomenų tvarkymo sutarčių

2.2.5 teisinius reikalavimus, susijusius su pranešimu apie incidentus, sąveika su teisėsauga ir tarptautiniu duomenų perdavimu

3. Tikslai

3.1 Užtikrinti, kad visi taikytini teisės aktai, reglamentai, standartai ir sutartiniai įpareigojimai būtų identifikuoti, dokumentuoti, išaiškinti ir įgyvendinti visoje organizacijoje.

3.2 Integruoti teisinius ir reguliacinius reikalavimus į organizacijos informacijos saugumo valdymo sistemą (ISVS), rizikos valdymo procesus, tiekėjų sutartis ir produktų bei paslaugų projektavimą.

3.3 Nustatyti mechanizmą, skirtą proaktyviai stebėti reguliacinius pokyčius ir atitinkamai atnaujinti kontrolės priemones bei dokumentaciją.

3.4 Apibrėžti aiškią atskaitomybę už atitikties priežiūrą, pažeidimų eskalavimą, išimčių valdymą ir išorinį ataskaitų teikimą.

3.5 Užtikrinti organizacijos teisinės ir reguliacinės atitikties būklės audituojamumą ir pagrįstumą patikrinimų, tyrimų ar sertifikavimo peržiūrų metu.

4. Vaidmenys ir atsakomybės

4.1 Vadovybė

4.1.1 Atsako už strateginę atskaitomybę dėl teisinės ir reguliacinės atitikties visos organizacijos mastu.

4.1.2 Peržiūri ir tvirtina didelės rizikos atitikties sprendimus, įskaitant rizikos prisiėmimą ir teisinius ginčus.

4.2 Atitikties pareigūnas / generalinis direktorius / teisininkas

4.2.1 Tvarko Atitikties įpareigojimų registrą, kuriame pateikiami visi taikytini teisės aktai, standartai, sertifikatai ir sutartinės nuostatos.

4.2.2 Atlieka teisinio poveikio vertinimus naujoms paslaugoms, rinkoms ar duomenų srautams.

4.2.3 Teikia autoritetingą teisės aktų ir standartų aiškinimą.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Metinė politikos peržiūra

9.1.1 Ši politika turi būti peržiūrima bent kartą per kalendorinius metus, siekiant:

9.1.1.1 užtikrinti nuolatinį suderinamumą su atnaujintais teisės aktais, pramonės standartais ir reguliacinėmis sistemomis

9.1.1.2 patvirtinti veiksmingumą remiantis audito išvadomis ir incidentų istorija

9.1.1.3 atspindėti organizacinius pokyčius (pvz., naujas jurisdikcijas, sistemas ar veiklos kryptis)

9.2 Peržiūros pagal suveikimo veiksnius

9.2.1 Tarpinės peržiūros turi būti inicijuojamos, kai:

9.2.2 priimamas arba atnaujinamas naujas teisinis ar reguliacinis reikalavimas

9.2.3 atitikties incidentas arba auditas atskleidžia politikos trūkumus

9.2.4 organizacija pradeda veiklą naujoje rinkoje ar paslaugų srityje, kuriai taikomos atskiros atitikties sistemos

9.2.5 taikymo praktikos tendencijos arba reguliavimo institucijų gairės rodo rizikos laikysenos pokyčius

9.3 Savininkystė ir tvirtinimas

9.3.1 Teisės departamentas ir Atitikties pareigūnas bendrai atsako už peržiūros proceso koordinavimą.

9.3.2 Galutiniai politikos pakeitimai turi būti patvirtinti vadovybės ir registruojami Politikos pakeitimų registre, nurodant susijusias pakeitimų kontrolės nuorodas ir komunikacijos planus.

9.4 Versijų kontrolė ir komunikacija

9.4.1 Bet kuri atnaujinta šios politikos versija turi:

9.4.1.1 apimti pagrindinių pakeitimų santrauką

9.4.1.2 būti pakartotinai išplatinta oficialiais kanalais (pvz., politikų portalas, LMS, vidiniai naujienlaiškiai)

9.4.1.3 reikalauti paveikto personalo patvirtinimo, ypač iš teisės, operacijų, saugumo ir tiekėjų valdymo vaidmenis vykdančių darbuotojų

10. Susijusios politikos ir sąsajos

10.1 Ši politika taikoma kartu su toliau nurodytomis organizacijos ISVS politikomis ir jas sustiprina:

10.1.1 P1 – Informacijos saugumo politika: nustato bazinius valdysenos principus, užtikrinančius, kad visos informacijos saugumo politikos, įskaitant atitiktį, būtų suderintos su strateginiais verslo ir reguliaciniais reikalavimais.

10.1.2 P2 – Valdysenos vaidmenų ir atsakomybių politika: apibrėžia sprendimų priėmimo įgaliojimus, įskaitant teisės ir atitikties vaidmenis, atsakingus už reguliacinę priežiūrą ir atskaitomybę.

10.1.3 P6 – Rizikos valdymo politika: padeda vertinti, priskirti savininkus ir mažinti teisinės bei reguliacinės atitikties rizikas visos organizacijos mastu.

10.1.4 P8 – Informacijos saugumo supratimo ir mokymo politika: užtikrina, kad visas personalas būtų informuotas apie atitikties atsakomybes ir gautų jų vaidmeniui tinkamus mokymus.

10.1.5 P12 – Turto valdymo politika: sustiprina teisinius įpareigojimus valdyti ir saugoti reguliuojamą arba sutartinį turtą, įskaitant asmens duomenis ir kritinę infrastruktūrą.

10.1.6 P30 – Reagavimo į incidentus politika: reglamentuoja privalomus teisinius pranešimus (pvz., BDAR 33 straipsnį) ir eskalavimo procedūras atitikties pažeidimo ar reguliacinio įvykio atveju.

10.1.7 P33 – Audito ir atitikties stebėsenos politika: nustato struktūruotas užtikrinimo veiklas, įskaitant kontrolės priemonių testavimą ir įrodymų rinkimą, reikalingas vidaus ir išorės atitikties patvirtinimui.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 4.2 punktas – Suinteresuotųjų šalių poreikių ir lūkesčių supratimas: reikalauja identifikuoti ir integruoti teisinius bei reguliacinius reikalavimus į ISVS.

11.1.2 5.1 punktas – Lyderystė ir įsipareigojimas: nustato vadovybės atskaitomybę už teisinės atitikties sukūrimą ir palaikymą visoje organizacijoje.

11.1.3 5.3 punktas – Organizaciniai vaidmenys, atsakomybės ir įgaliojimai: užtikrina vaidmenų aiškumą teisinei priežiūrai ir reguliacinei atitikčiai.

11.1.4 A priedo 5.36 kontrolės priemonė – Atitiktis teisiniams ir sutartiniams reikalavimams: nustato reikalavimą identifikuoti ir vykdyti iš teisės aktų, reglamentų ir sutarčių kylančius įpareigojimus.

11.2 ISO/IEC 27002

11.2.1 5.36 kontrolės priemonė: pateikia įgyvendinimo gaires, kaip tvarkyti atitikties įpareigojimų registrą, validuoti reguliacinius reikalavimus ir užtikrinti struktūruotą įrodymų saugojimą.

11.3 NIST SP 800-53 Rev.

11.3.1 PL-1 – Saugumo planavimo politika ir procedūros: reikalauja, kad atitikties reikalavimai būtų integruoti į valdysenos struktūras ir dokumentaciją.

11.3.2 PM-1 – Informacijos saugumo programos planas: nustato reguliacines kontrolės priemones kaip platesnės saugumo programos sudedamąją dalį.

11.3.3 CA-7 – Nuolatinė stebėsena: palaiko kontrolės priemonių veiksmingumo priežiūrą, užtikrinant teisinių ir politikos reikalavimų vykdymą.

11.3.4 AU-9 – Audito informacijos apsauga: užtikrina, kad atitikties audito žurnalai ir įrašai būtų apsaugoti ir prieinami patikrinimui.

11.4 ES BDAR (2016/679)

11.4.1 5 straipsnis – Su duomenų tvarkymu susiję principai: reikalauja teisėto tvarkymo, skaidrumo ir atskaitomybės.

11.4.2 6 straipsnis – Duomenų tvarkymo teisėtumas: nustato tinkamą teisinį pagrindą visoms duomenų tvarkymo veikloms.

11.4.3 24 straipsnis – Duomenų valdytojo atsakomybė: nustato tiesioginę atskaitomybę už reguliacinės atitikties užtikrinimą.

11.4.4 32 straipsnis – Tvarkymo saugumas: reikalauja įgyvendinti tinkamas technines ir organizacines priemones (TOM).

11.4.5 33 straipsnis – Pranešimas apie pažeidimą: reikalauja apie asmens duomenų saugumo pažeidimą pranešti atitinkamoms institucijoms per 72 valandas.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 20–21 straipsniai: reikalauja, kad esminiai ir svarbūs subjektai įgyvendintų dokumentuotą valdyseną, teisinės atitikties strategijas ir nuolatinę teisinių rizikų peržiūrą.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 5(2) straipsnis – IRT rizikos valdymo sistema: reikalauja integruoti teisinę atitiktį į platesnes rizikos valdymo ir priežiūros funkcijas.

11.6.2 19 straipsnis – IRT trečiųjų šalių rizika: nustato konkrečius teisinius reikalavimus, susijusius su sutartinių ir reguliacinių įpareigojimų valdymu, kai dalyvauja išorės tiekėjai ir platformos.

11.7 COBIT 2019

11.7.1 APO12 – Rizikos valdymas: įtraukia teisinę ir reguliacinę atitiktį kaip kritines įmonės rizikos valdysenos sudedamąsias dalis.

11.7.2 MEA03 – Atitikties išoriniams reikalavimams stebėsena: apibrėžia nuolatinę stebėseną, išimčių valdymą ir pasirengimą auditui visų formų reguliaciniams įpareigojimams.