					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P13					Dokumento pavadinimas: **Duomenų klasifikavimo ir ženklinimo 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 formalią organizacijos informacijos išteklių klasifikavimo ir ženklinimo sistemą, pagrįstą jautrumu, rizikos poveikiu ir reglamentavimo reikalavimais.

1.2 Ji užtikrina, kad visa informacija, nepriklausomai nuo to, ar ji saugoma, perduodama ar tvarkoma, būtų aiškiai suskirstyta į kategorijas ir paženklinta taip, kad būtų nurodytas jai taikomas apsaugos ir tvarkymo lygis.

1.3 Ši politika nustato struktūrizuotą klasifikavimo tvarką, suderintą su organizacijos rizikos valdymo praktika, ir padeda užtikrinti konfidencialumo, vientisumo ir prieinamumo tikslų įgyvendinimą tiek skaitmeninių, tiek fizinių duomenų atžvilgiu.

1.4 Ši kontrolės priemonė yra būtina siekiant užtikrinti vaidmenimis grindžiamą prieigą, pasirengimą auditui, tinkamą dalijimąsi duomenimis ir veiksmingą techninių apsaugos priemonių, tokių kaip šifravimas, atsarginės kopijos ir stebėsena, taikymą.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 Visiems organizacijos informacijos ištekliams, įskaitant dokumentus, duomenų bazes, įrašus ir komunikaciją

2.1.2 Visiems duomenų formatams, įskaitant skaitmeninį, spausdintinį, rašytinį ir žodinį

2.1.3 Visoms aplinkoms: vietinėms, nuotolinėms, mobiliosioms ir debesijos

2.1.4 Visiems darbuotojams, rangovams, paslaugų teikėjams ir trečiųjų šalių tvarkytojams, kurie kuria, tvarko ar saugo organizacijos informaciją

2.2 Taikymo sritis apima viduje sukurtą turinį, iš išorės gautus duomenis, asmens duomenis, kuriems taikomi privatumo teisės aktų reikalavimai (pvz., ES BDAR), ir informaciją, kuria keičiamasi su klientais, partneriais ir reguliavimo institucijomis.

2.3 Ji taikoma visoms sistemoms, naudojamoms duomenims saugoti ar perduoti, įskaitant įmonės taikomąsias programas, failų serverius, el. pašto sistemas, debesijos platformas ir atsarginių kopijų saugyklas.

3. Tikslai

3.1 Nustatyti standartizuotą, visai organizacijai taikomą klasifikavimo schemą, pagrįstą duomenų atskleidimo arba kompromitavimo poveikiu.

3.2 Užtikrinti, kad visa informacija būtų aiškiai, matomai ir nuosekliai ženklinama taip, kad ženklinimas atspindėtų jos klasifikavimo lygį ir tvarkymo reikalavimus.

3.3 Užtikrinti duomenų tvarkymo ir prieigos kontrolės priemones, suderintas su klasifikavimu, įskaitant šifravimą, žurnalų tvarkymą, perdavimo apsaugą ir saugojimo terminų nustatymą.

3.4 Užtikrinti atitiktį tarptautiniams standartams (ISO/IEC 27001, 27002), teisiniams pagrindams (ES BDAR, NIS2 direktyvai, DORA reglamentui) ir vidaus rizikos valdymo politikoms.

3.5 Užtikrinti, kad visi naudotojai suprastų savo atsakomybes saugant duomenis, taikant žymas ir tinkamai tvarkant klasifikuotą informaciją.

3.6 Užtikrinti atsekamumą tarp klasifikavimo būsenos, susijusių kontrolės priemonių ir organizacijos turto apskaitos audito ir atitikties tikslais.

4. Vaidmenys ir atsakomybės

4.1 Informacijos saugumo vadovas (CISO)

4.1.1 Valdo informacijos klasifikavimo ir ženklinimo politiką ir užtikrina jos suderinamumą su reglamentavimo, sutartiniais ir veiklos reikalavimais.

4.1.2 Tvirtina klasifikavimo lygius, ženklinimo standartus ir politikos pakeitimus.

4.1.3 Vykdo politikos laikymosi priežiūrą per auditus, metrikas ir išimčių peržiūras.

4.1.4 Koordinuoja tarpfunkcinę valdyseną su teisės, duomenų privatumo ir rizikos valdymo komandomis.

4.2 Informacijos išteklių savininkai

4.2.1 Atsako už jų valdomų informacijos išteklių klasifikavimą pagal organizacijos klasifikavimo schemą.

4.2.2 Taiko klasifikavimo žymas sukūrimo, atnaujinimo arba gavimo metu.

4.2.3 Periodiškai peržiūri turto klasifikavimą, ypač pasikeitus jautrumui, reglamentavimo taikymo sričiai arba verslo vertei.

4.2.4 Užtikrina, kad jautrūs duomenys būtų tinkamai tvarkomi ir ženklinami per visą jų gyvavimo ciklą.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Ši politika turi būti peržiūrima bent kartą per metus siekiant užtikrinti jos suderinamumą su:

9.1.1 Kintančiais reglamentavimo reikalavimais (pvz., ES BDAR, NIS2 direktyva, DORA reglamentas)

9.1.2 ISO/IEC 27001 arba 27002 klasifikavimo gairių atnaujinimais

9.1.3 Organizaciniais pokyčiais, turinčiais įtakos duomenų jautrumui arba savininkystei

9.1.4 Technologiniais pokyčiais, įskaitant naujas dokumentų arba duomenų valdymo platformas

9.2 Informacijos saugumo vadovas (CISO) turi inicijuoti peržiūrą bendradarbiaudamas su Informacijos saugumo valdymo komitetu, teisininkais ir paveiktais verslo padaliniais.

9.3 Peržiūros turi apimti:

9.3.1 Klasifikavimo taikymo veiksmingumą ir naudotojų laikymąsi

9.3.2 Incidentų arba išimčių, susijusių su neteisingu klasifikavimu, analizę

9.3.3 Naudotojų grįžtamąjį ryšį apie ženklinimo įrankius arba metodinę medžiagą

9.3.4 Palyginimą su pramonėje taikomais klasifikavimo standartais

9.4 Politikos atnaujinimai turi būti valdomi pagal versijų kontrolės reikalavimus, dokumentuojami ISVS saugykloje ir komunikuojami visam susijusiam personalui, akcentuojant naujas atsakomybes arba įrankių pokyčius.

9.5 Nauji darbuotojai turi būti supažindinami su galiojančia politikos versija įvedimo į darbą metu. Visi darbuotojai po reikšmingų politikos pakeitimų privalo baigti kvalifikacijos atnaujinimo mokymus.

10. Susijusios politikos ir sąsajos

10.1 Šią politiką tiesiogiai palaiko ir joje aprašytas kontrolės priemones sustiprina šios susijusios politikos:

10.1.1 P4 - Prieigos kontrolės politika: prieiga prie informacijos valdoma pagal klasifikavimo lygius; jautresniems duomenims reikalinga griežtesnė prieigos kontrolė ir autorizavimo mechanizmai.

10.1.2 P11 - Naudotojų paskyrų ir privilegijų valdymo politika: sustiprina privilegijų skyrimą pagal būtinybės žinoti principą, kuris nustatomas remiantis klasifikavimo lygiais.

10.1.3 P12 - Turto valdymo politika: užtikrina, kad kiekvienas turto apskaitoje esantis vienetas turėtų savo klasifikavimą ir žymą, taip palaikant atsekamumą ir atskaitomybę.

10.1.4 P14 - Duomenų saugojimo ir sunaikinimo politika: sunaikinimo ir saugojimo taisyklės nustatomos pagal duomenų klasifikavimo lygį ir reglamentavimo saugojimo reikalavimus.

10.1.5 P18 - Kriptografinių kontrolės priemonių politika: taiko tinkamus šifravimo standartus pagal informacijos ištekliaus klasifikavimą.

10.1.6 P22 - Žurnalų tvarkymo ir stebėsenos politika: sudaro sąlygas stebėti prieigą prie klasifikuotos informacijos ir jos judėjimą, užtikrinant audituojamumą ir neteisingo ženklinimo arba netinkamo naudojimo aptikimą.

10.2 Kiekviena sąsaja užtikrina nuoseklią informacijos apsaugą per visą jos gyvavimo ciklą – nuo sukūrimo ir klasifikavimo iki saugaus tvarkymo, saugojimo, perdavimo ir galutinio sunaikinimo.

11. Pamatiniai standartai ir sistemos

11.1 Ši politika suderinta su tarptautiniu mastu pripažintais standartais ir reglamentavimo sistemomis, reglamentuojančiomis jautrios informacijos klasifikavimą ir ženklinimą.

11.2 ISO/IEC 27001

11.2.1 4.2 punktas - Suinteresuotųjų šalių poreikių ir lūkesčių supratimas. Klasifikavimo reikalavimai dažnai kyla iš teisinių, reglamentavimo arba sutartinių įpareigojimų, kuriuos nustato suinteresuotosios šalys (pvz., ES BDAR, klientų konfidencialumo sutartys), ir tai turi būti atspindėta politikoje.

11.2.2 6.1.3 punktas - Informacijos saugos rizikos tvarkymas. Klasifikavimas tiesiogiai daro įtaką rizikos tvarkymo kontrolės priemonių parinkimui, įskaitant prieigos kontrolę, šifravimą ir saugojimą, pagal duomenų jautrumą.

11.2.3 7.2 punktas - Kompetencija. Politika nustato, kad už klasifikavimą ir ženklinimą atsakingas personalas turi būti apmokytas, todėl tai patenka į kompetencijos reikalavimų sritį.

11.2.4 7.3 punktas - Informuotumas. Politika reikalauja, kad visi naudotojai žinotų klasifikavimo lygius ir savo atsakomybes tvarkant informaciją, taip užtikrinant pareigų informuotumą saugumo srityje.

11.2.5 7.5 punktas - Dokumentuota informacija. Pati klasifikavimo politika yra kontroliuojamas dokumentas, o procedūros, mokymų įrašai ir klasifikavimo žymos yra dokumentuotos informacijos dalis.

11.2.6 8.1 punktas - Veiklos planavimas ir kontrolė. Klasifikavimas ir ženklinimas yra veiklos procesai, integruoti į duomenų gyvavimo ciklo valdymą, o šis punktas užtikrina, kad tokia veikla būtų suplanuota, įgyvendinta ir kontroliuojama.

11.2.7 9.1 punktas - Stebėsena, matavimas, analizė ir vertinimas. Politika apima nuostatas dėl klasifikavimo atitikties stebėsenos, incidentų tendencijų ir ženklinimo schemos veiksmingumo vertinimo.

11.2.8 10.1 punktas - Neatitiktis ir korekciniai veiksmai. Politika apibrėžia reagavimą į neteisingą klasifikavimą, įskaitant korekcinius veiksmus, tokius kaip pakartotiniai mokymai, atnaujinimai ir išimčių tvarkymas.

11.3 ISO/IEC 27002:2022

11.3.1 Kontrolė 5.12 - Informacijos klasifikavimas. Ši kontrolės priemonė užtikrina, kad informacija būtų klasifikuojama pagal jos jautrumą, vertę ir kritiškumą – būtent tai formalizuoja ši politika.

11.3.2 Kontrolė 5.13 - Informacijos ženklinimas. Ši kontrolės priemonė reikalauja tinkamai ženklinti informaciją pagal jos klasifikavimo lygį, o ši politika tai išsamiai nustato.

11.3.3 Kontrolė 5.10 - Informacijos ir kitų susijusių išteklių priimtinas naudojimas. Politika nustato, kaip naudotojai turi tvarkyti klasifikuotus duomenis, taip tiesiogiai palaikydama priimtiną organizacijos turto naudojimą ir užkirsdama kelią netinkamam naudojimui.

11.3.4 Kontrolė 5.11 - Turto grąžinimas. Klasifikavimas padeda užtikrinti, kad jautrūs duomenys būtų identifikuoti ir saugiai grąžinti arba išvalyti darbuotojui ar tiekėjui išvykstant.

11.3.5 Kontrolė 5.9 - Informacijos ir kitų susijusių išteklių apskaita. Klasifikavimas dažnai siejamas su turto apskaita, kurioje turi būti atspindėtas kiekvieno vieneto klasifikavimo lygis, kad būtų galima tinkamai priskirti kontrolės priemones.

11.3.6 Kontrolė 5.14 - Informacijos perdavimas. Klasifikavimo lygiai lemia vidaus ir išorinių duomenų perdavimo kontrolės priemones (pvz., šifravimą, patvirtinimą, prieigos apribojimus).

11.3.7 Kontrolė 8.12 - Duomenų nutekėjimo prevencija. Klasifikavimo ir ženklinimo taikymas padeda užkirsti kelią neteisėtam atskleidimui ir duomenų praradimui.

11.3.8 Kontrolė 8.11 - Duomenų maskavimas. Tam tikri klasifikavimo lygiai (pvz., Konfidencialus, Ribojamas) gali reikalauti maskavimo, kai duomenys naudojami testavimo, kūrimo arba analitikos tikslais.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Sistemų ir ryšių apsaugos politika ir procedūros: palaiko klasifikavimo politiką kaip bendrosios duomenų apsaugos dalį.

11.4.2 AC-16 - Saugumo atributai: įgyvendina prieigos užtikrinimą remiantis klasifikavimo metaduomenimis ir naudotojų leidimais.

11.4.3 MP-3 / MP-5 - Laikmenų žymėjimas ir transportavimo apsauga: užtikrina saugomų ir perduodamų duomenų ženklinimą ir apsaugą pagal klasifikavimą.

11.5 ES BDAR (2016/679)

11.5.1 5 straipsnis - Duomenų apsaugos principai: reikalauja, kad asmens duomenys būtų tvarkomi saugiai ir proporcingai jų jautrumui.

11.5.2 32 straipsnis - Tvarkymo saugumas: sustiprina klasifikavimą kaip rizika grindžiamą duomenų apsaugos mechanizmą ir tinkamų techninių priemonių taikymą.

11.6 ES NIS2 direktyva (2022/2555)

11.6.1 21(2)(a) straipsnis: reikalauja informacijos saugumo rizikos valdymo politikų, įskaitant turto ir duomenų klasifikavimo kontrolės priemones.

11.6.2 21(3) straipsnis: skatina taikyti priemones tinkamam duomenų tvarkymui užtikrinti – tai palaikoma klasifikavimu grindžiamu ženklinimu.

11.7 ES DORA reglamentas (2022/2554)

11.7.1 5 straipsnis - Valdysena ir kontrolė: reikalauja valdysenos sistemų, pagal kurias duomenų turtas klasifikuojamas IRT rizikos kontrolei.

11.7.2 9 straipsnis - IRT rizikos valdymas: nustato technines ir organizacines priemones kritiniams IRT ištekliams, įskaitant klasifikavimą ir ženklinimą.

11.8 COBIT 2019

11.8.1 DSS05.02 - Saugumo paslaugų valdymas: įtvirtina informacijos saugumo klasifikavimą siekiant užtikrinti įmonės duomenų apsaugą.

11.8.2 MEA03 - Atitikties stebėsena, vertinimas ir analizė: palaiko reguliarų klasifikavimo praktikos auditą ir peržiūrą, kad būtų užtikrintas politikos laikymasis ir branda.