					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P13S					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**

Suderinta su standartais ir reglamentais

Standartas / reglamentavimas	Punktas / straipsnis	Komentaras
ISO/IEC 27001:2022	5.3, 8 punktai	
ISO/IEC 27002:2022	Kontrolės priemonės 5.12, 5.13	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
ES NIS2 direktyva	21 straipsnio 2 dalies a punktas	
ES DORA reglamentas	5 straipsnio 8 dalis	
COBIT 2019	BAI03.05, DSS05	
ES BDAR	5, 32 straipsniai	

1. Tikslas

1.1 Ši politika nustato, kaip visa organizacijos tvarkoma informacija turi būti klasifikuojama ir ženklinama, siekiant užtikrinti jos konfidencialumą, vientisumą ir prieinamumą per visą gyvavimo ciklą.

1.2 Ji užtikrina nuoseklią duomenų tvarkymo praktiką, priskiriant informacijai tinkamus apsaugos lygius pagal jos jautrumą, poveikį veiklai arba teisinius reikalavimus.

1.3 Klasifikavimas ir ženklinimas padeda mažinti atsitiktinio atskleidimo, neteisėtos prieigos ar netinkamo jautrių duomenų tvarkymo riziką, ypač mažose ir vidutinėse įmonėse, kurios gali naudoti paprastesnes sistemas ir turėti mažiau formalizuotų kontrolės priemonių.

1.4 Ši politika yra svarbi ISO/IEC 27001 sertifikavimui ir atitikčiai taikomiems reglamentavimo reikalavimams, ypač duomenų apsaugos teisės aktams, tokiems kaip ES BDAR, ir kibernetinio saugumo sistemoms, tokioms kaip NIS2 direktyva ir DORA reglamentas.

2. Taikymo sritis

2.1 Ši politika taikoma visiems organizacijos duomenims, nepriklausomai nuo jų formato ar vietos, įskaitant:

2.1.1 elektroninius dokumentus, skaičiuokles, el. laiškus, formas, vaizdus ir nuskenuotus failus;

2.1.2 fizinius dokumentus, tokius kaip spausdinti įrašai, ataskaitos, sąskaitos ir užrašai;

2.1.3 duomenis, saugomus ar tvarkomus debesijos paslaugose, vietiniuose serveriuose, keičiamose laikmenose arba veikloje naudojamuose asmeniniuose įrenginiuose;

2.1.4 laikinuosius ar tarpinius duomenis, sukuriamus vykdant veiklą (pvz., žurnalus, podėlio failus, el. laiškus).

2.2 Visi darbuotojai, rangovai, laikinieji darbuotojai ir išorės paslaugų teikėjai, turintys prieigą prie organizacijos duomenų, privalo laikytis šios politikos.

2.3 Ši politika taikoma visam duomenų gyvavimo ciklui – nuo sukūrimo ir saugojimo iki prieigos suteikimo, perdavimo, archyvavimo ar ištrynimo.

3. Tikslai

3.1 Nustatyti paprastą ir įgyvendinamą klasifikavimo schemą, kuri būtų lengvai suprantama ir taikoma visoje organizacijoje.

3.2 Reikalauti, kad kiekvienas duomenų išteklius būtų klasifikuojamas pagal jo jautrumą ir atitinkamai ženklinamas, siekiant užtikrinti tinkamą jo tvarkymą, saugojimą ir prieigą.

3.3 Užtikrinti, kad duomenų ženklinimo praktika būtų integruota į veiklos procesus, tokius kaip darbuotojų įvedimas, projektų inicijavimas ir sistemų parengimas.

3.4 Mažinti duomenų saugumo pažeidimų riziką, taikant tvarkymo kontrolės priemones (pvz., šifravimą, prieigos apribojimus) pagal klasifikavimo lygį.

3.5 Užtikrinti atitiktį privatumo ir informacijos saugumo teisės aktams, parodant, kad jautrūs duomenys (pvz., asmens, finansiniai ar nuosavybiniai duomenys) yra tinkamai ženklinami ir valdomi.

3.6 Nustatyti atskaitomybę už klasifikavimo sprendimus ir užtikrinti periodinę peržiūrą bei atnaujinimus pagal kintančius veiklos ir teisinius poreikius.

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas (GV)

4.1.1 Atsako už šią politiką ir tvirtina klasifikavimo schemą.

4.1.2 Užtikrina priežiūrą, kad atsakomybės už klasifikavimą būtų deleguotos ir įgyvendinamos.

4.1.3 Privalo peržiūrėti ir patvirtinti visas išimtis, susijusias su klasifikavimo ar ženklinimo reikalavimais.

4.1.4 Užtikrina, kad duomenų tvarkymo praktika atitiktų tokių teisės aktų kaip ES BDAR ir DORA reglamentas reikalavimus.

4.2 Informacijos savininkas / duomenų valdytojas

4.2.1 Sukūrus ar įsigijus kiekvieną naują duomenų rinkinį ar informacijos išteklių, priskiria jam pradinį klasifikavimo lygį.

4.2.2 Užtikrina, kad, kai taikoma, būtų naudojamos matomos žymos (pvz., failų antraštės, poraštės, vandens ženklai, aplankų pavadinimai).

4.2.3 Periodiškai peržiūri klasifikavimą, siekdamas patvirtinti jo aktualumą, tikslumą ir nustatyti būtinus pakeitimus (pvz., po išslaptinimo ar paskelbimo).

4.2.4 Kartu su IT vadovu užtikrina techninių apsaugos priemonių taikymą pagal klasifikavimo lygį (pvz., prieigos teisės, šifravimas).

[... 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 kasmet peržiūrima GV ir duomenų valdytojo, siekiant užtikrinti, kad ji atspindėtų:

9.1.1 veiklos procesų arba duomenų tipų pokyčius;

9.1.2 naujus reglamentavimo reikalavimus (pvz., susijusius su duomenų privatumu arba finansine priežiūra);

9.1.3 technologinius pokyčius, darančius įtaką ženklinimo arba klasifikavimo galimybėms.

9.2 Peržiūra turi apimti klasifikavimo kategorijų, ženklinimo priemonių ar praktikos bei informuotumo ir mokymų turinio atnaujinimus.

9.3 Politikos pakeitimai turi būti patvirtinti GV ir komunikuoti visam personalui. Audito tikslais turi būti saugomas versijų keitimų registras.

10. Susijusios politikos ir sąsajos

10.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: nustato atskaitomybę už politikos savininkystę ir jos įgyvendinimą.

10.2 P4S – Prieigos kontrolės politika: suderina sistemų prieigą su duomenų klasifikavimo lygiais.

10.3 P12S – Turto valdymo politika: sudaro sąlygas sekti fizinį ir skaitmeninį turtą, kuriame saugomi klasifikuoti duomenys.

10.4 P17S – Duomenų apsaugos ir privatumo politika: reglamentuoja asmens duomenų, kurių didelė dalis klasifikuojama kaip „Konfidenciali“, apsaugą.

10.5 P30S – Reagavimo į incidentus politika: nustato eskalavimo tvarką ir reagavimo procedūras klasifikavimo pažeidimų arba duomenų atskleidimo atvejais.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 5.3 punktas: reikalauja aiškiai apibrėžtų atsakomybių už duomenų tvarkymą ir apsaugą.

11.1.2 8.1 punktas: nustato veiklos planavimo ir kontrolės reikalavimus, įskaitant reikalavimus, susijusius su duomenų kategorizavimu.

11.2 ISO/IEC 27002

11.2.1 Kontrolės priemonė 5.12: pateikia gaires dėl informacijos klasifikavimo pagal riziką ir reglamentavimo reikalavimus.

11.2.2 Kontrolės priemonė 5.13: detalizuoja praktinius ženklinimo mechanizmus ir susijusias tvarkymo taisykles.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: reikalauja žymėti informaciją, kad apsaugos priemonės atitiktų klasifikavimo lygį.

11.3.2 MP-3 / MP-5: pateikia gaires dėl laikmenų ir išvesčių ženklinimo bei kontrolės.

11.4 ES BDAR

11.4.1 5 ir 32 straipsniai: nustato duomenų kiekio mažinimo ir vientisumo užtikrinimo reikalavimus, taikant tinkamą klasifikavimą ir duomenų tvarkymo apsaugos priemones.

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies a punktas: nustato techninių ir organizacinių kontrolės priemonių taikymą rizika grindžiamai duomenų apsaugai.

11.6 ES DORA reglamentas

11.6.1 5 straipsnio 8 dalis: reikalauja, kad įmonės klasifikuotų duomenų išteklius kaip savo IRT rizikos valdymo programos dalį.

11.7 COBIT 2019

11.7.1 BAI03.05: numato informacijos klasifikavimą ir pagal riziką pritaikytą apsaugą.

11.7.2 DSS05.02: apima klasifikavimu grindžiamų kontrolės priemonių taikymą ir stebėseną.