					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P14S					Dokumento pavadinimas: **Duomenų saugojimo ir sunaikinimo 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	Pastaba
ISO/IEC 27001:2022	6.1.3, 8 skyriai	Apima rizikos valdymą, operacines kontrolės priemones ir saugojimo reikalavimus
ISO/IEC 27002:2022	Kontrolė 5	Gairės dėl saugojimo terminų ir saugaus sunaikinimo metodų
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Audito įrašų saugojimas, laikmenų sanitarinis išvalymas, duomenų saugojimo ribos ir jų taikymas
ES NIS2 direktyva	21 straipsnio 2 dalies a punktas	Reikalaujama riziką atitinkanti gyvavimo ciklo valdymo politika
ES DORA reglamentas	5 straipsnio 1 dalis	IRT rizikos valdymas: duomenų prieinamumas ir pašalinimas
COBIT 2019	BAI03.04, DSS01	Informacijos gyvavimo ciklo kontrolės priemonės, saugus sunaikinimas
ES BDAR	5 straipsnio 1 dalies e punktas, 17 straipsnis	Duomenys saugomi ne ilgiau, nei būtina; teisė ištrinti

1. Tikslas

1.1 Šios politikos tikslas – nustatyti privalomas taisykles, reglamentuojančias informacijos saugojimą ir saugų sunaikinimą MVĮ aplinkoje. Ji užtikrina, kad įrašai būtų saugomi tik tiek, kiek to reikalauja teisės aktai, sutartiniai įsipareigojimai ar verslo poreikiai, o vėliau būtų saugiai sunaikinami.

1.2 Šia politika siekiama mažinti informacijos saugumo riziką, valdyti teisinę riziką ir riboti perteklinį ar pasenusį duomenų saugojimą. Ji padeda užtikrinti atitiktį ISO/IEC 27001 ir privatumo sistemoms, tokioms kaip ES BDAR, mažinant neteisėtą asmens ar jautrios informacijos saugojimą.

1.3 Tinkamai struktūruota saugojimo ir sunaikinimo sistema mažina veiklos sąnaudas, gerina sistemų našumą ir stiprina pasirengimą auditui. MVĮ, kurių IT pajėgumai riboti, ši politika suteikia praktišką būdą atsakingai valdyti skaitmeninius ir fizinius informacijos išteklius.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 visiems organizacijos sukurtiems, surinktiems, tvarkomiems ar saugomiems įrašams, byloms, žurnalams, komunikacijai ir duomenų rinkiniams;

2.1.2 visiems darbuotojams, rangovams ir išorės paslaugų teikėjams, tvarkantiems organizacijos duomenis;

2.1.3 visiems duomenų formatams (pvz., popieriniams, elektroniniams, vaizdo, garso ar žurnalų duomenims) ir visoms saugojimo laikmenoms (pvz., vietiniams diskams, debesijos paslaugoms, el. pašto serveriams, atsarginėms kopijoms).

2.2 Taikymo sritis apima:

2.2.1 veiklos dokumentus (pvz., sąskaitas faktūras, sutartis, projektų ataskaitas);

2.2.2 operacinius įrašus (pvz., žurnalus, prieigos istoriją, atsarginių kopijų momentines kopijas);

2.2.3 asmens duomenis (pvz., personalo bylas, klientų komunikaciją, pagalbos įrašus);

2.2.4 duomenis, saugomus vidinėse, išorinėse arba hibridinėse aplinkose;

2.2.5 archyvinius ir atsarginių kopijų duomenis, nepriklausomai nuo to, ar jie aktyvūs, ar neaktyvūs.

2.3 Į taikymo sritį įtraukiami visi duomenų gyvavimo ciklo etapai – nuo sukūrimo iki autorizuoto sunaikinimo.

3. Tikslai

3.1 Nustatyti nuoseklias saugojimo taisykles, pagrįstas teisiniais, veiklos ir reguliaciniais kriterijais.

3.2 Užkirsti kelią per ankstyvam kritinių įrašų ištrynimui ir pašalinti nereikalingą duomenų kaupimą.

3.3 Užtikrinti saugų ir negrįžtamą duomenų sunaikinimą, kai jų saugojimas nebereikalingas.

3.4 Priskirti atsakomybę už saugojimo ir ištrynimo sprendimų įgyvendinimą, atsižvelgiant į MVĮ personalo išteklių ribotumą.

3.5 Užtikrinti auditui parengtą dokumentaciją, leidžiančią pagrįsti deramą rūpestingumą pagal ISO 27001, ES BDAR, NIS2 direktyvą ir kitas sistemas.

3.6 Skatinti saugų duomenų tvarkymą per visą gyvavimo ciklą, nesukuriant nepagrįstos techninės naštos ne specialistams.

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas (GV)

4.1.1 Tvirtina šią politiką ir atsako už jos valdymą.

4.1.2 Užtikrina, kad saugojimo ir sunaikinimo procedūros būtų įgyvendinamos laikantis teisinių ir verslo rizikos reikalavimų.

4.1.3 Kai būtina, tvirtina išimtis ir teisinį sulaikymą.

4.1.4 Inicijuoja politikos peržiūras ir tvirtina atnaujinimus, atsižvelgdamas į verslo ar reguliavimo pokyčius.

4.2 Paskirtasis duomenų savininkas

4.2.1 Skiriamas kiekvienai duomenų kategorijai (pvz., finansų, žmogiškųjų išteklių, klientų įrašų).

4.2.2 Klasifikuoja įrašus ir nustato tinkamą saugojimo terminą pagal šią politiką ir teisinius reikalavimus.

4.2.3 Tvirtina ištrynimą, kai saugojimo reikalavimai yra įvykdyti.

4.2.4 Padeda atlikti vidaus auditus, pateikdamas kontekstą apie saugojimo logiką ir sunaikinimo įvykius.

[... 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 arba įvykus bent vienai iš šių aplinkybių:

9.1.1 pasikeitus taikomiems teisės aktams (pvz., duomenų privatumo, finansinės atskaitomybės srityje);

9.1.2 pradėjus taikyti naujas sistemas ar procesus, darančius poveikį duomenų gyvavimo ciklui;

9.1.3 gavus audito išvadas arba įvykus incidentams, atskleidžiantiems saugojimo praktikos spragas.

9.2 Peržiūrų metu turi būti užtikrinta, kad Saugojimo registras išliktų išsamus ir apimtų visas pagrindines įrašų kategorijas.

9.3 Politikos atnaujinimus turi patvirtinti Generalinis vadovas, o paveiktas personalas turi būti apie juos informuotas. Naujausia versija turi būti prieinama ir valdoma pagal versijų kontrolės reikalavimus.

10. Susijusios politikos ir sąsajos

10.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: apibrėžia politikos valdymą ir įgaliojimus tvirtinti išimtis.

10.2 P13S – Duomenų klasifikavimo ir ženklinimo politika: nustato, kaip saugojimo taisyklės derinamos su duomenų klasifikavimu.

10.3 P12S – Turto valdymo politika: reglamentuoja saugojimo laikmenas, kuriose yra duomenų, kuriems taikomi saugojimo ir sunaikinimo reikalavimai.

10.4 P17S – Duomenų apsaugos ir privatumo politika: užtikrina duomenų apsaugą ir minimizavimą bei palaiko teisėtą tvarkymą pagal ES BDAR.

10.5 P30S – Reagavimo į incidentus politika: taikoma, kai dėl sunaikinimo ar saugojimo nesėkmių kyla galimas duomenų atskleidimas.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 6.1.3 skyrius: reikalaujama valdyti su informacija susijusias rizikas, įskaitant saugojimo rizikas.

11.1.2 8.1 skyrius: apibrėžia gyvavimo ciklo operacines kontrolės priemones.

11.2 ISO/IEC 27002

11.2.1 Kontrolė 5.33: gairės dėl saugojimo terminų nustatymo ir saugaus sunaikinimo metodų.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: reikalaujamas audito įrašų saugojimas.

11.3.2 MP-6: apibrėžia laikmenų sanitarinio išvalymo procedūras.

11.3.3 SI-12: apima duomenų saugojimo ribas ir jų taikymą.

11.4 ES BDAR

11.4.1 5 straipsnio 1 dalies e punktas: duomenys turi būti saugomi ne ilgiau, nei būtina.

11.4.2 17 straipsnis: teisė ištrinti taikoma, kai duomenys nebėra teisėtai saugomi.

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies a punktas: reikalaujama riziką atitinkančių organizacinių politikų, įskaitant gyvavimo ciklo valdymą.

11.6 ES DORA reglamentas

11.6.1 5 straipsnio 1 dalis: IRT rizikos valdymas apima duomenų prieinamumą ir pašalinimą.

11.7 COBIT 2019

11.7.1 BAI03.04: reikalaujamos informacijos gyvavimo ciklo kontrolės priemonės.

11.7.2 DSS01.06: saugaus sunaikinimo procedūros kaip informacijos išteklių apsaugos dalis.