					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P14					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	Punktas / straipsnis	Komentaras
ISO/IEC 27001:2022	6.1.3, 8.1 punktai	
ISO/IEC 27002:2022	Kontrolės priemonės 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
ES BDAR	5(1)(e), 17, 32 straipsniai	
ES NIS2 direktyva	21(2)(a-e) straipsnis	
ES DORA reglamentas	5, 9 straipsniai	
COBIT 2019	DSS01, DSS05, MEA	

1. Tikslas

1.1 Šios politikos tikslas – nustatyti organizacinius duomenų saugojimo ir saugaus sunaikinimo reikalavimus visuose informacijos gyvavimo ciklo etapuose. Ji užtikrina atitiktį taikomiems teisiniams, reguliavimo ir sutartiniams įpareigojimams bei padeda išvengti nereikalingo ar rizikingo duomenų kaupimo.

1.2 Ši politika padeda įgyvendinti ISO/IEC 27001:2022 reikalavimus, nustatydama duomenų saugojimo trukmės kontrolę ir negrįžtamo sunaikinimo praktiką. Ji užtikrina atsekamą įrašų dokumentavimą, nustato su klasifikavimo jautrumu suderintus saugojimo reikalavimus ir palaiko pasirengimą auditui, reguliuotojų patikrinimams ir teisinio atskleidimo procesams.

1.3 Be to, šia politika siekiama užtikrinti duomenų konfidencialumą, vientisumą ir prieinamumą, kartu mažinant verslo riziką, veiklos neefektyvumą ir privatumo pažeidimų riziką, kylančią dėl netinkamo duomenų saugojimo ar sunaikinimo.

2. Taikymo sritis

2.1 Ši politika taikoma visam fiziniam ir skaitmeniniam turtui, kurį organizacija valdo, tvarko ar saugo, įskaitant turtą, esantį trečiųjų šalių, patronuojamųjų įmonių ar išorinių paslaugų teikėjų kontrolėje.

2.2 Taikymo sritis apima, be kita ko:

2.2.1 Dokumentus, failus ir įrašus (skaitmeninius ir popierinius)

2.2.2 Duomenų bazes ir archyvus

2.2.3 El. laiškus ir momentinių pranešimų žurnalus

2.2.4 Atsargines kopijas, sistemų žurnalus ir audito seką

2.2.5 Pirminį kodą, taikomųjų programų duomenis ir debesijos turtą

2.2.6 Keičiamąsias laikmenas ir pasenusią aparatinę įrangą, kurioje yra duomenų

2.3 Ši politika reglamentuoja tiek operacinius įrašus, tiek reguliuojamus duomenų rinkinius (pvz., finansinius, teisinius, žmogiškųjų išteklių, su klientais susijusius ir auditui svarbius duomenis), nepriklausomai nuo saugojimo vietos ar sistemos.

2.4 Ji taikoma visiems organizacijos padaliniams, darbuotojams, rangovams ir tiekėjams, kurie dalyvauja kuriant, saugant, valdant ar sunaikinant duomenis.

3. Tikslai

3.1 Užtikrinti, kad duomenys būtų saugomi tik tiek laiko, kiek būtina pagal teisės aktų, sutarčių ar veiklos reikalavimus, o nebereikalingi duomenys būtų saugiai sunaikinami.

3.2 Užkirsti kelią per ankstyvam, neleistinam ar atsitiktiniam įrašų, reikalingų veiklai vykdyti, atitikčiai užtikrinti, bylinėjimuisi ar auditui, ištrynimui.

3.3 Nustatyti ir taikyti nuoseklius saugojimo terminus pagal informacijos klasifikaciją, turto tipą, taikomus teisės aktus ir rizikos lygį.

3.4 Apsaugoti duomenų privatumą ir konfidencialumą jų saugojimo laikotarpiu ir sunaikinimo metu, įskaitant duomenų subjektų teisių įgyvendinimą (pvz., ištrynimą pagal BDAR 17 straipsnį).

3.5 Užtikrinti, kad visi duomenų sunaikinimo metodai būtų negrįžtami, tinkamai dokumentuoti ir atitiktų pripažintus standartus, pvz., NIST SP 800-88.

3.6 Mažinti veiklos neefektyvumą, papildomas sąnaudas ir teisinę riziką, kylančią dėl perteklinio saugojimo ar neapskaitytų senųjų duomenų.

3.7 Palaikyti veiklos tęstinumo ir atkūrimo po incidentų tikslus, taikant integruotą atsarginių kopijų saugojimo valdyseną ir pagrįstą duomenų archyvavimo praktiką.

4. Vaidmenys ir atsakomybės

4.1 Vadovybė

4.1.1 Tvirtina šią politiką ir užtikrina tinkamą finansavimą, išteklius bei integravimą į įmonės rizikos valdymo ir atitikties programas.

4.1.2 Prisiima bendrą atskaitomybę už teisinę ir reguliavimo atitiktį, susijusią su duomenų saugojimu ir saugiu sunaikinimu.

4.2 Informacijos saugumo vadovas (CISO)

4.2.1 Yra šios politikos savininkas ir atsako už duomenų saugojimo bei sunaikinimo valdysenos nustatymą ir peržiūrą, suderintą su informacijos saugumo valdymo sistema (ISVS).

4.2.2 Užtikrina, kad klasifikacija grindžiami saugojimo ir sunaikinimo reikalavimai būtų įgyvendinti verslo padaliniuose ir techninėse sistemose.

4.2.3 Stebi politikos laikymąsi ir prireikus inicijuoja korekcinius veiksmus.

[... 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 kasmet arba kai tenkinama bent viena iš šių sąlygų:

9.1.1 Pasikeičia taikomi teisės aktai ar reguliavimo reikalavimai, darantys poveikį duomenų saugojimui (pvz., BDAR, mokesčių taisyklių ar DORA reglamento atnaujinimai)

9.1.2 Peržiūrima klasifikavimo sistema ar verslo procesai, darantys poveikį duomenų gyvavimo ciklo etapams

9.1.3 Įdiegiamos naujos IT sistemos, archyvavimo platformos ar laikmenų sunaikinimo technologijos

9.1.4 Vidaus audito išvados ar reguliuotojų rekomendacijos parodo saugojimo ar sunaikinimo praktikos spragas

9.2 Peržiūrai turi vadovauti CISO ir duomenų apsaugos pareigūnas (DAP), dalyvaujant teisininkams, atitikties, IT ir verslo padaliniams.

9.3 Pagrindinis duomenų saugojimo terminų sąrašas (MDRS) ir sunaikinimo registras turi būti peržiūrimi lygiagrečiai, siekiant užtikrinti, kad:

9.3.1 Terminai išliktų tikslūs ir atspindėtų veiklos, teisinius bei reguliavimo poreikius

9.3.2 Sunaikinimo dokumentacija būtų išsami ir tinkama auditui

9.3.3 Teisinio sulaikymo įrašai būtų patvirtinti ir, kai tinkama, panaikinti

9.4 Bet kokie politikos atnaujinimai privalo:

9.4.1 Būti formaliai valdomi pagal versijų kontrolę ir saugomi ISVS dokumentų saugykloje

9.4.2 Apimti peržiūrų istoriją ir pakeitimų pagrindimą

9.4.3 Būti patvirtinti vadovybės

9.4.4 Būti komunikuojami atitinkamam personalui kartu su atnaujinta mokymų ar gairių medžiaga

9.5 Įvykus reikšmingiems politikos pakeitimams, paveikti darbuotojai per 30 dienų nuo paskelbimo privalo baigti tikslinius mokymus, kad būtų užtikrintas tolesnis atitikties laikymasis.

9.6 Susijusios politikos ir sąsajos

10. Susijusios politikos ir sąsajos

10.1.1 P4 - Prieigos kontrolės politika: užtikrina, kad duomenis jų saugojimo laikotarpiu pasiektų tik įgalioti asmenys, o pasibaigusio termino duomenims iki sunaikinimo būtų taikomi apribojimai.

10.1.2 P12 - Turto valdymo politika: nustato, kuris turtas turi duomenų, kuriems reikalingas planinis sunaikinimas, ir seka jų gyvavimo ciklą nuo įsigijimo iki sunaikinimo.

10.1.3 P13 - Duomenų klasifikavimo ir ženklinimo politika: nustato klasifikavimo sprendimų gaires, tiesiogiai lemiančias duomenų saugojimo trukmę ir reikiamą sunaikinimo metodą.

10.1.4 P15 - Atsarginių kopijų ir atkūrimo politika: apibrėžia atsarginių kopijų laikmenų ir replikuotų duomenų išteklių saugojimo terminus bei sunaikinimo procedūras.

10.1.5 P18 - Kriptografinių kontrolės priemonių politika: palaiko kriptografinį ištrynimą sunaikinimo tikslais ir užtikrina duomenų šifravimą saugojimo metu iki sunaikinimo.

10.1.6 P30 - Reagavimo į incidentus politika: taikoma tais atvejais, kai dėl netinkamo sunaikinimo kyla galimas duomenų praradimas, pažeidimas ar reguliavimo neatitiktis.

10.2 Kiekviena susijusi politika padeda užtikrinti nuoseklų duomenų valdysenos modelį klasifikavimo, gyvavimo ciklo kontrolės, prieigos ir pasirengimo auditui srityse.

11. Pamatiniai standartai ir sistemos

11.1 Ši politika yra suderinta su tarptautiniu mastu pripažintais standartais ir reguliavimo sistemomis, kurios apibrėžia saugią, atitiktį užtikrinančią ir veiksmingą duomenų gyvavimo ciklo praktiką.

11.2 ISO/IEC 27001:

11.2.1 6.1.3 punktas - Rizikos valdymo planas: palaiko rizikų, susijusių su pertekliniu saugojimu, duomenų saugumo pažeidimais ar sunaikinimo nesėkmėmis, mažinimą.

11.2.2 8.1 punktas - Veiklos planavimas ir kontrolė: nustato gyvavimo ciklo kontrolės priemones, reglamentuojančias saugojimą, archyvavimą ir sunaikinimą.

11.3 ISO/IEC 27002:2022 - Kontrolės priemonės 5.10, 5.12, 5.30, 5: pateikia praktines gaires dėl priimtino duomenų naudojimo, saugojimo pagrindimo, kontroliuojamo ištrynimo ir pagrįsto įrašų tvarkymo pagal organizacijos rizikos toleranciją.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Audito įrašų saugojimas: užtikrina pakankamą audito žurnalų ir atitikties įrodymų saugojimą.

11.4.2 MP-6 - Laikmenų išvalymas: reikalauja saugių, dokumentuotų fizinių ir elektroninių laikmenų sunaikinimo metodų.

11.4.3 SI-12 - Informacijos tvarkymas: nustato tinkamą duomenų tvarkymą pagal saugojimo ir sunaikinimo kontrolės priemones.

11.4.4 PL-2 - Sistemos saugumo ir privatumo planas: reikalauja dokumentuoti sistemai taikomas duomenų gyvavimo ciklo valdymo ir saugaus sunaikinimo nuostatas.

11.5 ES BDAR (2016/679):

11.5.1 5(1)(e) straipsnis - duomenų kiekio mažinimas ir saugojimo trukmės ribojimas: reikalauja, kad duomenys nebūtų saugomi ilgiau, nei būtina.

11.5.2 17 straipsnis - teisė į ištrynimą („teisė būti pamirštam“): reikalauja operatyvaus ir galutinio asmens duomenų ištrynimo gavus pagrįstą prašymą.

11.5.3 32 straipsnis - tvarkymo saugumas: sustiprina duomenų apsaugą saugojimo metu ir reikalauja saugaus nebegaliojančių įrašų sunaikinimo.

11.6 ES NIS2 direktyva (2022/2555):

11.6.1 21(2)(a-e) straipsnis: reikalauja, kad subjektai taikytų politikas ir technines priemones saugiam duomenų tvarkymui, įskaitant saugojimo ribojimą ir sunaikinimo metodus.

11.7 ES DORA reglamentas (2022/2554):

11.7.1 5 straipsnis - valdysena ir kontrolė: nustato struktūruotą IRT rizikos valdymą, įskaitant saugų informacijos gyvavimo ciklo valdymą.

11.7.2 9 straipsnis - IRT rizikos valdymo sistema: reikalauja politikų dėl duomenų saugojimo, sunaikinimo ir skaitmeninių operacijų teisinės bei reguliavimo atitikties.

11.8 COBIT 2019:

11.8.1 DSS01 - Valdomos operacijos: palaiko saugojimo stebėseną ir nuoseklumą visose duomenų sistemose.

11.8.2 DSS05 - Valdomos saugumo paslaugos: užtikrina saugomų ir archyvuotų duomenų apsaugą iki saugaus sunaikinimo.

11.8.3 MEA03 - Stebėti, vertinti ir analizuoti atitiktį: sudaro galimybes audituoti saugojimo reikalavimų taikymą, ištrynimo procedūras ir reguliavimo reikalavimų įvykdymą.