					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: P16					Dokumento pavadinimas: **Duomenų maskavimo ir pseudoniminimo 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 punktai	Bendrieji rizikos valdymo ir operacinių kontrolės priemonių reikalavimai, taikomi maskavimui ir pseudoniminimui
ISO/IEC 27002:2022	Kontrolės priemonės 8.11, 8	Kontrolės gairės dėl maskavimo ir pseudoniminimo įgyvendinimo
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Privatumo ir konfidencialumo kontrolės priemonės, skirtos duomenų minimizavimui, transformavimui ir prieigos ribojimui
ES BDAR	4(5), 5(1)(c,f), 32 straipsniai	Pseudoniminimo ir duomenų apsaugos priemonių teisinis pagrindas ir reikalavimai
ES NIS2 direktyva	21(2)(c) straipsnis	Pareiga taikyti technines ir organizacines priemones, įskaitant privatumą didinančias technologijas (PET)
ES DORA reglamentas	10(1), 10(2)(e) straipsniai	IRT rizikos valdymo ir konfidencialumo kontrolės priemonės, taikomos duomenų maskavimui ir pseudoniminimui
COBIT 2019	DSS05.01, DSS06.06, MEA	Valdysenos kontrolės priemonės, skirtos duomenų apsaugai taikant maskavimą ir vertinant atitiktį

1. Tikslas

1.1 Ši politika apibrėžia organizacijos požiūrį į duomenų maskavimo ir pseudoniminimo, kaip privatumą didinančių technologijų (PET), įgyvendinimą, siekiant sumažinti asmens duomenų ar jautrių duomenų identifikuojamumą ir atskleidimo riziką.

1.2 Ji padeda užtikrinti saugų informacijos naudojimą testavimo, analitikos ir operacinėje veikloje, laikantis teisinių ir reguliavimo reikalavimų, mažinant duomenų saugumo pažeidimų poveikį ir taikant duomenų minimizavimo bei konfidencialumo principus.

1.3 Politika suderinta su ISO/IEC 27001:2022, remia ES BDAR 4(5) straipsnio nuostatas dėl pseudoniminimo ir apima rizika grindžiamą įgyvendinimą, atitinkantį NIST, NIS2 direktyvos, DORA reglamento ir COBIT 2019 reikalavimus.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 visiems darbuotojams, rangovams, trečiosioms šalims ir tiekėjams, turintiems prieigą prie sistemų, kuriose tvarkoma asmeninė, konfidenciali ar jautri informacija;

2.1.2 visoms duomenų aplinkoms, įskaitant produkcinę, kūrimo, testavimo ir parengiamąją aplinką;

2.1.3 visoms duomenų maskavimo formoms (pvz., statiniam, dinaminiam, deterministiniam maskavimui, žetonizacijai) ir pseudoniminimo metodams, naudojamiems privatumo rizikai mažinti;

2.1.4 visų tipų duomenims (struktūrizuotiems ir nestruktūrizuotiems), sistemoms (vietinėms ar debesijos) ir taikomosioms programoms, susijusioms su asmens duomenimis ar reguliuojamais duomenimis.

2.2 Taikymo sritis apima naudojimą:

2.2.1 taikomųjų programų kūrimo ir kokybės užtikrinimo (QA) / testavimo aplinkose;

2.2.2 analitikos ar ataskaitų teikimo platformose;

2.2.3 keičiantis duomenimis su trečiosiomis šalimis ar paslaugų teikėjais;

2.2.4 atsarginių kopijų, archyvavimo ar atkūrimo sistemose.

3. Tikslai

3.1 Užtikrinti nuoseklų ir veiksmingą maskavimo ir pseudoniminimo taikymą, siekiant sumažinti duomenų atskleidimo ar netinkamo naudojimo riziką.

3.2 Užtikrinti, kad tikri duomenys niekada nebūtų naudojami neprodukcinėje aplinkoje, nebent jie būtų transformuoti taikant patvirtintas PET priemones.

3.3 Kai to reikia operaciniam nuoseklumui užtikrinti, išlaikyti referencinį vientisumą, tinkamumą naudoti ir formatą išsaugančias transformacijas.

3.4 Taikyti griežtą prieigos kontrolę pradiniams duomenims, maskuotiems duomenims ir pakartotinio identifikavimo raktams.

3.5 Maskuotus ar pseudonimintus duomenų rinkinius laikyti jautriais duomenimis, kuriems taikomas prieigos žurnalų vedimas, saugojimo kontrolės priemonės ir reagavimo į incidentus procedūros.

3.6 Patvirtinti šių kontrolės priemonių veiksmingumą vykdant nuolatinį testavimą, stebėseną ir audito procedūras.

4. Vaidmenys ir atsakomybės

4.1 Vadovybė

4.1.1 Tvirtina šią politiką ir užtikrina jos taikymą kaip platesnės IT valdysenos ir duomenų apsaugos iniciatyvų dalį.

4.2 Informacijos saugumo vadovas (CISO) / ISVS vadovas

4.2.1 Prižiūri įgyvendinimą ir nuolatinę atitiktį.

4.2.2 Užtikrina atitiktį ISO/IEC 27001 6.1.3 punktui (rizikos tvarkymas) ir 8.1 punktui (operacinė kontrolė).

4.2.3 Peržiūri audito žurnalus ir patvirtina kontrolės priemonių veiksmingumą.

[... 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 ne rečiau kaip kartą per metus arba anksčiau, jei įvyksta bent viena iš šių aplinkybių:

9.1.1 reguliavimo pokyčiai, darantys poveikį maskavimui arba pseudoniminimui;

9.1.2 naujų IT sistemų, tvarkančių jautrius duomenis, įdiegimas;

9.1.3 esminiai organizacijos duomenų klasifikavimo schemos pokyčiai;

9.1.4 audito išvados, rodančios kontrolės priemonių trūkumus;

9.1.5 naujų grėsmių arba maskavimo technologijų atsiradimas.

9.2 ISVS vadovas turi vadovauti peržiūrai, konsultuodamasis su duomenų apsaugos pareigūnu (DAP), duomenų savininkais, IT saugumo komanda ir teisine funkcija. Atnaujinimai turi būti valdomi pagal versijų kontrolės reikalavimus, patvirtinti aukščiausiosios vadovybės ir perduoti visoms susijusioms suinteresuotosioms šalims.

10. Susijusios politikos ir sąsajos

10.1 P13 - Duomenų klasifikavimo ir ženklinimo politika. Sprendimai dėl maskavimo ir pseudoniminimo tiesiogiai priklauso nuo P13 apibrėžto duomenų laukų klasifikavimo ir jautrumo lygių.

10.2 P14 - Duomenų saugojimo ir sunaikinimo politika. Transformuoti duomenų rinkiniai turi būti saugomi ir sunaikinami pagal P14 nustatytas gyvavimo ciklo taisykles, užtikrinant, kad maskuoti ir pseudoniminti duomenys būtų laikomi jautriais.

10.3 P17 - Duomenų apsaugos ir privatumo politika. Nustato privatumo principus ir reguliavimo pagrindą pseudoniminimui taikyti kaip reikalavimus atitinkančiai duomenų tvarkymo veiklai pagal ES BDAR ir panašius teisės aktus.

10.4 P22 - Žurnalų tvarkymo ir stebėsenos politika. Užtikrina centralizuotą maskavimo ir pseudoniminimo įvykių auditą ir įspėjimų valdymą pagal struktūrizuotus saugumo stebėsenos procesus.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 6.1.3 punktas - Rizikos tvarkymo planas: nustato maskavimą ir pseudoniminimą kaip rizikos tvarkymo mechanizmus, skirtus sumažinti jautrių duomenų identifikuojamumą neesminio tvarkymo aplinkose.

11.1.2 8.1 punktas - Operacinis planavimas ir kontrolė: nustato technines ir procedūrines kontrolės priemones saugiam duomenų transformavimui tvarkymo, saugojimo ar perdavimo metu.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrolės priemonės 8.11, 8: gairės dėl duomenų maskavimo ir pseudoniminimo, siekiant sumažinti pakartotinio identifikavimo ir nutekėjimo riziką.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - AII apsauga: privatumą didinančių technologijų, tokių kaip maskavimas ir pseudoniminimas, įgyvendinimas.

11.3.2 PT-2, PT-3 - AII tvarkymo minimizavimas ir saugumas: transformavimas, skirtas sumažinti identifikuojamumą ir taikyti prieigos kontrolę.

11.3.3 SC-12, SC-28, SC-30 - Duomenų konfidencialumas ir vientisumas: konfidencialumo ir užtemdymo kontrolės priemonės saugojimui, perdavimui ir naudojimui.

11.4 ES BDAR (2016/679)

11.4.1 4(5) straipsnis: formalus pseudoniminimo apibrėžimas.

11.4.2 32 straipsnis: tvarkymo saugumas - organizacinės ir techninės pseudoniminimo priemonės.

11.4.3 5(1)(c,f) straipsnis: duomenų minimizavimas ir konfidencialumas taikant pseudoniminimą / maskavimą.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21(2)(c) straipsnis: reikalauja taikyti PET priemones, tokias kaip maskavimas ir pseudoniminimas, kaip saugumo priemones.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 10(1) straipsnis: IRT rizikos valdymo sistema apima maskavimo / pseudoniminimo kontrolės priemones.

11.6.2 10(2)(e) straipsnis: nustato pareigą naudoti transformavimo technologijas asmens ir finansiniams duomenims apsaugoti.

11.7 COBIT 2019

11.7.1 DSS05.01 - Informacijos išteklių apsauga: maskavimo ir pseudoniminimo reikalavimai.

11.7.2 DSS06.06 - Saugus testavimas ir analitika: maskavimas aplinkose už produkcinės aplinkos ribų.

11.7.3 MEA03 - atitikties stebėsena, skirta maskavimo ir pseudoniminimo veiksmingumui vertinti.