					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P24S					Dokumento pavadinimas: **Saugaus kūrimo 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	8 punktas	Aktualios informacijos saugumo kontrolės priemonės operacinei veiklai, įskaitant saugų kūrimą
ISO/IEC 27002:2022	Kontrolės priemonės 8.25–8.27	Apima saugaus kūrimo gyvavimo ciklą, testavimą ir trečiųjų šalių kūrėjų saugumo atsakomybes
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Apima saugų SDLC, prieigos kontrolę ir pažeidžiamumų valdymą kūrimo procese
ES BDAR	25 straipsnis	Reikalauja užtikrinti duomenų apsaugą pagal projektavimą ir pagal numatytuosius nustatymus programinės įrangos kūrimo procese
ES NIS2 direktyva	21 straipsnio 2 dalies a, e, h punktai	Nustato pareigą taikyti saugaus kūrimo politikas, vykdyti atvirojo kodo priežiūrą ir dokumentuoti rizikos mažinimo priemones
ES DORA reglamentas	6 straipsnio 7 dalis, 9 straipsnio 1 dalies c punktas, 10 straipsnio 2 dalies c punktas	Kritinių IRT sistemų gyvavimo ciklo saugumas finansų sektoriuje
COBIT 2019	BAI	Sistema struktūrizuotam, atsekamam ir atspariam saugaus kūrimo valdymui

1. Tikslas

1.1 Ši politika užtikrina, kad visa programinė įranga, scenarijai ir žiniatinkliu grindžiami įrankiai, kuriuos organizacija arba jos išorės partneriai kuria ar modifikuoja, būtų kuriami saugiai, mažinant pažeidžiamumų, neteisėtos prieigos prie duomenų ir veiklos sutrikimų riziką.

1.2 Joje nustatomos privalomos saugaus kūrimo taisyklės ir saugaus programavimo praktikos, kurių privalo laikytis visi vidiniai kūrėjai, rangovai ir tiekėjai, nepriklausomai nuo projekto dydžio ar sudėtingumo.

1.3 Ši politika skirta apsaugoti klientų duomenis, užkirsti kelią duomenų saugumo pažeidimams ir užtikrinti, kad organizacijos vardu ar jos naudai sukurta arba pritaikyta programinė įranga atitiktų saugumo audito reikalavimus, taikomus teisinius reikalavimus (pvz., ES BDAR, NIS2 direktyvą, DORA reglamentą) ir padėtų palaikyti ISO/IEC 27001 sertifikavimą.

2. Taikymo sritis

2.1 Ši politika taikoma visiems asmenims ir subjektams, kurie organizacijos vardu dalyvauja kuriant, pritaikant, diegiant ar valdant toliau nurodytus objektus:

2.1.1 interneto svetaines, taikomąsias programas arba automatizavimo įrankius;

2.1.2 organizacijos viduje sukurtus scenarijus arba programinę įrangą;

2.1.3 kodą, kurį sukuria trečiųjų šalių kūrėjai arba laisvai samdomi specialistai;

2.1.4 papildinius, bibliotekas ir programinės įrangos komponentus, integruotus į produkcines sistemas.

2.2 Ji apima visas kūrimo veiklai naudojamas aplinkas, įskaitant:

2.2.1 kūrimo ir testavimo aplinkas;

2.2.2 parengiamąją ir priešprodukcinę aplinką;

2.2.3 produkcines sistemas, naudojamas individualiai sukurtam kodui vykdyti.

2.3 Ši politika taip pat reglamentuoja duomenų tvarkymą kūrimo ir diegimo metu, ypač kai produkciniai duomenys naudojami neprodukcinėje aplinkoje.

3. Tikslai

3.1 Užkirsti kelią saugumo trūkumų ar pažeidžiamumų įtraukimui į individualiai kuriamą arba trečiųjų šalių sukurtą programinę įrangą.

3.2 Užtikrinti, kad saugaus programavimo praktika ir pažeidžiamumų prevencija būtų integruotos į kiekvieną programinės įrangos kūrimo gyvavimo ciklo etapą.

3.3 Sumažinti riziką, susijusią su atvirojo kodo ar trečiųjų šalių komponentų naudojimu, nustatant privalomą jų tinkamą patikrą ir apskaitą.

3.4 Nustatyti privalomą formalų kodo peržiūros ir taikomųjų programų saugumo testavimo atlikimą prieš išleidimą.

3.5 Kontroliuoti prieigą prie kūrimo aplinkų ir užtikrinti jų atskyrimą nuo veikiančių produkcinių sistemų.

3.6 Užtikrinti atitiktį privalomiems tarptautinių standartų ir reglamentų reikalavimams (pvz., ISO/IEC 27001, ES BDAR, DORA reglamentui, NIS2 direktyvai).

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas (GM)

4.1.1 Tvirtina šią politiką ir yra jos savininkas.

4.1.2 Užtikrina, kad visas programinės įrangos kūrimas, vykdomas viduje ar perduotas išorei, atitiktų šią politiką.

4.1.3 Peržiūri ir pasirašo kūrimo ar paslaugų sutartis, kuriose įtrauktos saugaus kūrimo nuostatos.

4.1.4 Tikrina tiekėjų atitiktį reguliarių peržiūrų metu arba pareikalaudamas saugumo įrodymų.

4.2 Vidinis kūrėjas arba taikomosios programos savininkas

4.2.1 Laikosi saugaus programavimo ir diegimo praktikos.

4.2.2 Kiekvienam projektui taiko saugaus kūrimo kontrolinį sąrašą.

4.2.3 Patvirtina visų naudojamų atvirojo kodo ar trečiųjų šalių komponentų saugumą.

4.2.4 Nedelsdamas praneša GM apie visus nustatytus pažeidžiamumus.

[... 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 Generalinio vadovo peržiūrima bent kartą per metus siekiant:

9.1.1 patikrinti nuolatinę atitiktį ISO/IEC 27001, ES BDAR, NIS2 direktyvos ir DORA reglamento reikalavimams;

9.1.2 atspindėti atnaujintas grėsmes arba saugaus kūrimo gerosios praktikos pokyčius;

9.1.3 užtikrinti suderinamumą su bet kokiais naujais įrankiais, platformomis ar tiekėjų santykiais.

9.2 Tarpinės peržiūros turi būti inicijuojamos, kai įvyksta bent viena iš šių aplinkybių:

9.2.1 pranešama apie bet kokį programinės įrangos saugumo incidentą;

9.2.2 įdiegiama nauja kūrimo sistema arba prieglobos platforma;

9.2.3 pasikeičia trečiųjų šalių kūrimo partneriai;

9.2.4 įsigalioja reguliavimo pokyčiai, darantys poveikį programinės įrangos ar saugumo įsipareigojimams.

9.3 Visi šios politikos pakeitimai privalo būti:

9.3.1 dokumentuoti, nurodant datą, pakeitimo santrauką ir GM patvirtinimą;

9.3.2 aiškiai komunikuoti visam vidiniam ir išoriniam kūrimo personalui;

9.3.3 saugomi kaip organizacijos versijų kontrolės ir versijų istorijos dalis.

9.4 Atnaujintos versijos turi būti lengvai prieinamos per vidines platformas, spausdintą dokumentaciją arba tiekėjams prieinamas debesijos paslaugas.

10. Susijusios politikos ir sąsajos

10.1 Ši politika palaiko kelių kitų SME politikų veiksmingą įgyvendinimą ir yra su jomis susieta:

10.1.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: nustato atskaitomybę už kūrimo saugumo kontrolės priemonių priskyrimą ir patikrinimą projektuose bei tiekėjų atžvilgiu.

10.1.2 P4S – Prieigos kontrolės politika: nustato bazines taisykles, kaip riboti prieigą prie kūrimo aplinkų ir kodo saugyklų, įskaitant pareigų atskyrimą (SoD).

10.1.3 P8S – Informacijos saugumo supratimo ir mokymo politika: užtikrina, kad vidiniai kūrėjai ir rangovai suprastų saugaus programavimo praktiką ir susijusias saugumo atsakomybes.

10.1.4 P17S – Duomenų apsaugos ir privatumo politika: paaiškina, kaip kūrimo, testavimo ir žurnalų tvarkymo procesuose turi būti tvarkomi asmens duomenys, kad būtų užtikrinta atitiktis ES BDAR.

10.1.5 P30S – Reagavimo į incidentus politika: apibrėžia, kaip su kūrimu susiję saugumo incidentai turi būti pranešami, vertinami ir šalinami, įskaitant su kodu susijusius atskleidimo atvejus.

10.2 Visos šios politikos kartu užtikrina, kad saugus kūrimas būtų įgyvendinamas ir patikrinamas net mažoje arba netechninėje organizacijoje.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8.1 punktas – reikalauja įgyvendinti operacines kontrolės priemones, įskaitant saugų kūrimą, suderintas su verslo tikslais ir rizikos tolerancija.

11.2 ISO/IEC 27002

11.2.1 Kontrolės priemonė 8.25 – rekomenduoja integruoti saugumą į visą programinės įrangos gyvavimo ciklą, įskaitant pirminio kodo kontrolę, versijų kontrolę ir kūrėjų prieigą.

11.2.2 Kontrolės priemonė 8.26 – nurodo taikomųjų programų testavimo metodus ir saugumo funkcionalumo patvirtinimą prieš paleidimą į produkcinę aplinką.

11.2.3 Kontrolės priemonė 8.27 – reikalauja, kad trečiųjų šalių kūrėjai laikytųsi tų pačių kūrimo standartų ir kad jų saugumo atsakomybės būtų aiškiai apibrėžtos.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3–SA-15 – apibrėžia saugaus kūrimo procesus, įskaitant kūrėjų prieigos kontrolę, testavimą, grėsmių modeliavimą ir dokumentavimą.

11.3.2 SI-10 – reikalauja, kad kūrėjai nustatytų ir mažintų įprastus programinės įrangos trūkumus bei, kai taikoma, naudotų automatizuotas priemones.

11.4 ES BDAR (2016/679)

11.4.1 25 straipsnis – „duomenų apsauga pagal projektavimą ir pagal numatytuosius nustatymus“ įpareigoja integruoti saugumo ir privatumo apsaugos priemones programinės įrangos projektavimo ir kūrimo metu, ypač kai tvarkomi asmens duomenys.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21 straipsnio 2 dalies a, e ir h punktai – reikalauja saugaus kūrimo politikų, atvirojo kodo naudojimo priežiūros ir dokumentuoto su taikomosiomis programomis susijusių rizikų mažinimo esminiuose ir svarbiuose subjektuose.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 6 straipsnio 7 dalis, 9 straipsnio 1 dalies c punktas ir 10 straipsnio 2 dalies c punktas – nustato kūrimo gyvavimo ciklo saugumo įsipareigojimus finansų sektoriaus subjektams, įskaitant MVĮ, ypač kritinėms IRT sistemoms.

11.7 COBIT 2019

11.7.1 BAI03 – „Sprendimų identifikavimo ir kūrimo valdymas“ palaiko struktūrizuotų kūrimo kontrolės priemonių įgyvendinimą, akcentuojant saugumą, atsekamumą ir atsparumą, pritaikytą MVĮ apribojimams.