					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P24					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**

1. Tikslas

1.1 Ši politika nustato privalomuosius saugumo reikalavimus organizacijos programinės įrangos ir sistemų kūrimo veikloms, įskaitant vidinį kūrimą, išorinį kūrimą ir trečiųjų šalių kodo integravimą.

1.2 Tikslas – užtikrinti, kad saugumas būtų integruotas per visą programinės įrangos kūrimo gyvavimo ciklą (SDLC) ir kad pažeidžiamumai būtų nustatomi, mažinami ir užkertamas kelias jų perkėlimui į gamybinę aplinką.

1.3 Ši politika padeda įgyvendinti ISO/IEC 27001:2022 8.1 skyriaus ir A priedo 8.25–8.28 kontrolės priemonių reikalavimus, standartizuojant saugaus kūrimo valdyseną, kodo validavimo praktiką ir trečiųjų šalių kūrimo priežiūrą.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 viduje arba išorėje kuriamai programinei įrangai, taikomosioms programoms, scenarijams, integracijoms ir automatizavimo priemonėms;

2.1.2 kūrimo komandoms, produktų savininkams, „DevOps“ specialistams, kokybės užtikrinimo specialistams, architektams, projektų vadovams ir rangovams;

2.1.3 SDLC aplinkoms, įskaitant kūrimo, testavimo, parengiamąsias ir priešgamybines sistemas;

2.1.4 atvirojo kodo ir trečiųjų šalių komponentams, integruojamiems į vidines taikomąsias programas;

2.1.5 programinei įrangai, diegiamai vietinėje infrastruktūroje, privačiosios debesijos, hibridinėse ar viešosios debesijos aplinkose.

2.2 Visi naudotojai ir subjektai, dalyvaujantys sistemų kūrime, testavime ar diegime organizacijos kontekste, įskaitant valdomųjų paslaugų teikėjus (MSP) ir platformų tiekėjus, privalo laikytis šios politikos.

3. Tikslai

3.1 Integruoti saugumo kontrolės priemones į visus programinės įrangos kūrimo etapus – nuo projektavimo iki diegimo, užtikrinant, kad rizikos mažinimas būtų aktyvus ir tęstinis.

3.2 Užkirsti kelią išnaudojamų pažeidžiamumų atsiradimui, tokių kaip įterpimo pažeidžiamumai, nesaugus autentifikavimas ir žinomų trečiųjų šalių trūkumų poveikis.

3.3 Nustatyti ir taikyti saugaus programavimo praktiką, suderintą su OWASP, SANS CWE ir konkrečioms platformoms taikomomis gairėmis.

3.4 Užtikrinti, kad visas kodas prieš diegimą būtų peržiūrėtas kolegų, patikrintas automatizuotomis priemonėmis ir kad būtų atliktas saugumo validavimas.

3.5 Valdyti kūrimo rizikas, kylančias dėl išorinio kūrimo, trečiųjų šalių kodo įtraukimo ir pakartotinio atvirojo kodo programinės įrangos naudojimo.

3.6 Apsaugoti kūrimo, testavimo ir parengiamąsias aplinkas nuo neteisėtos prieigos ir užkirsti kelią gamybinių duomenų naudojimui be patvirtinto duomenų maskavimo arba anonimizavimo.

3.7 Stiprinti kūrėjų, produktų vadovų ir kokybės užtikrinimo specialistų saugumo suvokimą, taikant vaidmenimis grindžiamus mokymus ir nuolat teikiant informaciją apie naujas grėsmes.

4. Vaidmenys ir atsakomybės

4.1 Informacijos saugumo vadovas (CISO)

4.1.1 Valdo šią politiką ir užtikrina, kad saugaus kūrimo reikalavimai būtų taikomi visoje organizacijoje.

4.1.2 Tvirtina saugaus programavimo standartus ir trečiųjų šalių kūrimo susitarimus.

4.1.3 Tvirtina rizikos tvarkymo sprendimus dėl neišspręstų arba atidėtų pažeidžiamumų.

4.2 Taikomųjų programų saugumo vadovas / „DevSecOps“ vadovas

4.2.1 Rengia, prižiūri ir užtikrina saugaus programavimo gairių taikymą.

4.2.2 Integruoja statinį ir dinaminį saugumo testavimą į CI/CD konvejerius.

4.2.3 Atlieka kodo saugumo peržiūras ir nustato privalomuosius taisomuosius 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 dažniau, jei įvyksta:

9.1.1 esminiai kūrimo metodikų arba „DevOps“ priemonių pakeitimai;

9.1.2 esminiai saugumo incidentai, kylantys dėl taikomųjų programų pažeidžiamumų;

9.1.3 reglamentavimo reikalavimų, susijusių su saugia programine įranga, pakeitimai (pvz., ES BDAR, DORA reglamentas);

9.1.4 nauji pramonės standartai arba grėsmių žvalgybos duomenys (pvz., OWASP Top 10, SLSA, MITRE CWE).

9.2 Politikos peržiūrai turi vadovauti Taikomųjų programų saugumo vadovas, koordinuodamas veiklą su CISO, programinės įrangos architektais, kokybės užtikrinimo vadovybe ir teisininku (kai tai susiję su trečiųjų šalių kodo pasekmėmis).

9.3 Bet kokie pakeitimai turi būti registruojami ISVS dokumentų registre, valdomi taikant versijų kontrolę ir komunikuojami paveiktoms komandoms per išleidimo pastabas arba privalomuosius mokymus.

9.4 Ankstesnės versijos turi būti saugomos archyvinėje saugykloje siekiant užtikrinti teisinį ir audito atsekamumą.

10. Susijusios politikos ir sąsajos

10.1 P1 – Informacijos saugumo politika. Nustato strateginį reikalavimą integruoti saugumą į visas informacines sistemas, o saugus kūrimas yra viena iš pagrindinių operacinių kontrolės priemonių.

10.2 P4 – Prieigos kontrolės politika. Apibrėžia kontrolės priemones, skirtas riboti prieigą prie kūrimo aplinkų, saugyklų, kūrimo priemonių ir CI/CD konvejerių.

10.3 P5 – Pakeitimų valdymo politika. Užtikrina, kad kodo pakeitimams, laidoms ir diegimams būtų taikomas tinkamas tvirtinimas, grąžinimo į ankstesnę būseną planavimas ir patikra po diegimo.

10.4 P12 – Turto valdymo politika. Palaiko kūrimo aplinkų, pirminio kodo saugyklų ir kūrimo sistemų apskaitą kaip valdomą turtą, kuriam taikomas klasifikavimas ir apsauga.

10.5 P22 – Žurnalų tvarkymo ir stebėsenos politika. Taikoma kūrimo konvejeriams, užtikrinant, kad kūrimo procesai, kodo perkėlimai ir diegimo įvykiai būtų registruojami, stebimi ir analizuojami dėl saugumo anomalijų.

10.6 P30 – Reagavimo į incidentus politika. Nustato sistemą saugumo trūkumams, nustatytiems po diegimo arba taikomųjų programų saugumo testavimo metu, analizuoti ir valdyti.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8.1 skyrius – Operacijų planavimas ir kontrolė: reikalauja į operacijas integruoti saugaus kūrimo procesus ir kontrolės priemones.

11.2 ISO/IEC 27002:2022 – Kontrolės priemonės 8.25–8.28

11.2.1 A priedo kontrolės priemonė 8.25 – saugaus kūrimo gyvavimo ciklas: reikalauja formaliai įtraukti saugumą į programinės įrangos projektavimą ir kūrimą.

11.2.2 A priedo kontrolės priemonė 8.26 – taikomųjų programų saugumo reikalavimai: reikalauja apibrėžti saugaus programavimo ir saugumo priėmimo kriterijus.

11.2.3 A priedo kontrolės priemonė 8.27 – saugi sistemų architektūra ir inžineriniai principai: reikalauja taikyti saugaus projektavimo principus ir mažinti žinomus trūkumus.

11.2.4 A priedo kontrolės priemonė 8.28 – saugus programavimo kodavimas: reikalauja taikyti saugaus programavimo praktiką programinės įrangos kūrimo metu.

11.3 NIST SP 800-53 5 redakcija

11.3.1 SA-3–SA-15: nustato struktūruotą taikomųjų programų saugumo kūrimo praktiką, įskaitant projektavimo, kodo vientisumo ir testavimo reikalavimus.

11.3.2 SI-10 – informacijos įvesties validavimas: apima saugaus programavimo apsaugos priemones.

11.3.3 SR-3 – tiekimo grandinės apsauga: reikalauja vertinti trečiųjų šalių programinę įrangą, komponentus ir kūrimo paslaugų teikėjus.

11.4 ES BDAR (2016/679)

11.4.1 25 straipsnis – duomenų apsauga pagal projektavimą ir numatytuosius nustatymus: reikalauja integruoti saugumą ir privatumą į sistemų kūrimą.

11.4.2 32 straipsnis – tvarkymo saugumas: pagrindžia technines priemones, tokias kaip įvesties validavimas, prieigos kontrolė ir saugus diegimas.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21 straipsnio 2 dalies e–f punktai: reikalauja programinės įrangos kūrimo praktikos, apimančios pažeidžiamumų valdymą, kodo saugumą ir incidentų pranešimą.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 9 straipsnis – IRT rizikos valdymas: reikalauja saugaus kūrimo praktikos finansų sektoriaus subjektams, įskaitant programinės įrangos kokybės kontrolės priemones ir trūkumų šalinimą.

11.6.2 10 straipsnis – veiklos tęstinumas ir testavimas: skatina griežtą IRT sistemų, įskaitant taikomąsias programas, testavimą ir validavimą.

11.7 COBIT 2019

11.7.1 BAI03 – sprendimų identifikavimo ir kūrimo valdymas: reglamentuoja projektavimą, kūrimą ir saugumo integravimą į naujus sprendimus.

11.7.2 BAI07 – pakeitimų priėmimo ir perėjimo valdymas: užtikrina saugų diegimą ir vertinimą po diegimo.

11.7.3 DSS05 – saugumo paslaugų valdymas: taikomas saugumo validavimui programinės įrangos ir paslaugų teikimo srityje.