					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P28					Dokumento pavadinimas: **Išorinio 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	Skyrius / straipsnis	Komentaras
ISO/IEC 27001:2022	8.1 skyrius	Netaikoma
ISO/IEC 27002:2022	Kontrolės priemonės 5.19–5.22, 8	Netaikoma
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	Netaikoma
ES BDAR	28, 32 straipsniai	Netaikoma
ES NIS2 direktyva	21(2)(a), (h), 23 straipsniai	Netaikoma
ES DORA reglamentas	28(1), (2) straipsniai	Netaikoma
COBIT 2019	APO10, BAI03, DSS	Netaikoma

1. Tikslas

1.1 Ši politika nustato privalomas kontrolės priemones, taikomas perduodant programinės įrangos ar sistemų kūrimą išorės tiekėjams, rangovams ar agentūroms, siekiant užtikrinti, kad saugios praktikos būtų integruotos visame kūrimo gyvavimo cikle.

1.2 Ja siekiama užkirsti kelią saugumo pažeidžiamumams, duomenų praradimui, intelektinės nuosavybės (IP) atskleidimui ir atitikties pažeidimams, kylantiems dėl išorinio kūrimo paslaugų.

1.3 Ši politika nustato tiekėjų valdysenos, saugaus programavimo, prieigos valdymo, stebėsenos pareigas ir prieigos bei bendradarbiavimo nutraukimo procesą pasibaigus sutarčiai, siekiant užtikrinti kuriamos programinės įrangos konfidencialumą, vientisumą ir prieinamumą.

2. Taikymo sritis

2.1 Ši politika taikoma visiems organizacijos padaliniams, kurie programinės įrangos ar sistemų kūrimui pasitelkia išorės subjektus, įskaitant:

2.1.1 žiniatinklio taikomąsias programas, mobiliąsias programėles, įterptąsias sistemas, taikomųjų programų sąsajas, scenarijus, automatizuotas darbo eigas ar platformų modulius;

2.1.2 individualų kūrimą vidinėms platformoms, klientams skirtoms sistemoms ar komerciniams produktams;

2.1.3 bendradarbiavimą su trečiųjų šalių programuotojais, laisvai samdomais specialistais, agentūromis ar užsienyje veikiančiomis komandomis.

2.2 Ši politika taip pat taikoma visiems išorės subjektams, kurie kūrimo metu gauna prieigą prie pirminio kodo, testavimo aplinkų ar CI/CD konvejerių.

2.3 Reikalavimai yra privalomi nepriklausomai nuo sutarties tipo, kūrimo metodikos ar išorės paslaugų teikėjo geografinės vietos.

3. Tikslai

3.1 Užtikrinti, kad visiems išorinio kūrimo atvejams nuo planavimo iki validavimo po diegimo būtų taikomos saugaus programinės įrangos kūrimo gyvavimo ciklo (SDLC) praktikos.

3.2 Užtikrinti, kad visose sutartyse su išorės programuotojais būtų įtrauktos privalomos nuostatos dėl duomenų apsaugos, saugaus programavimo ir intelektinės nuosavybės išsaugojimo.

3.3 Nustatyti prieigos kontrolės, stebėsenos ir audito reikalavimus trečiųjų šalių programuotojams, dirbantiems su vidinėmis sistemomis.

3.4 Apsaugoti organizaciją nuo tiekimo grandinės grėsmių, teisės aktų pažeidimų ir reputacijos žalos, susijusios su išorėje kuriama programine įranga.

3.5 Užtikrinti nuolatinę atitiktį saugumo sistemoms ir reglamentams, įskaitant ISO/IEC 27001, NIST, ES BDAR, NIS2 direktyvą, DORA reglamentą ir COBIT 2019.

4. Vaidmenys ir atsakomybės

4.1 Vadovybė

4.1.1 Tvirtina didelės rizikos išorinio kūrimo projektus ir pagrįstais atvejais patvirtina politikos išimtis.

4.1.2 Užtikrina, kad sprendimai dėl paslaugų perdavimo išorei atitiktų strateginius tikslus ir organizacijos rizikos apetitą.

4.2 Informacijos saugumo vadovas (CISO)

4.2.1 Tvirtina tiekėjų įtraukimą saugumo požiūriu.

4.2.2 Nustato saugumo kontrolės priemonių reikalavimus išorinio kūrimo atvejams ir peržiūri incidentų ataskaitas.

[... 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 dažniau šiomis aplinkybėmis:

9.1.1 įdiegus naujus kūrimo perdavimo išorei modelius, įtraukus naujus tiekėjus ar naujas jurisdikcijas;

9.1.2 atnaujinus reglamentavimo sistemas, tokias kaip ES BDAR, NIS2 direktyva ar DORA reglamentas;

9.1.3 po saugumo incidento, susijusio su išorėje sukurtu kodu, prieiga ar rezultatais;

9.1.4 pagal audito išvadas arba vykdant ISVS tobulinimą.

9.2 Informacijos saugumo vadovas (CISO) atsako už politikos peržiūros inicijavimą ir koordinavimą, konsultuodamasis su:

9.2.1.1 teisės ir pirkimų funkcijomis (dėl sutartinių nuostatų taikymo suderinimo);

9.2.1.2 projektų ir produktų savininkais (dėl veiklos įgyvendinamumo);

9.2.1.3 informacijos saugos funkcija (dėl grėsmių ir kontrolės priemonių atnaujinimų);

9.2.1.4 vadovybe (dėl galutinio tvirtinimo).

9.3 Visi politikos atnaujinimai turi būti:

9.3.1.1 valdomi taikant versijų kontrolę ir saugomi paskirtoje dokumentų saugykloje;

9.3.1.2 komunikuojami suinteresuotosioms šalims, dalyvaujančioms išorinio kūrimo veiklose;

9.3.1.3 susieti su susijusių politikų ar procedūrinės dokumentacijos atnaujinimais.

9.4 Prie kiekvienos politikos versijos turi būti pridedamas pakeitimų žurnalas, užtikrinantis pakeitimų ir patvirtinimų atsekamumą.

10. Susijusios politikos ir sąsajos

10.1 Ši politika palaiko toliau nurodytus susijusius dokumentus ir yra jų palaikoma:

10.1.1 P1 - Informacijos saugumo politika: nustato organizacijos lygmens saugumo principus, taikomus vidinio ir trečiųjų šalių kūrimo kontekstuose.

10.1.2 P5 - Pakeitimų valdymo politika: užtikrina, kad visi diegimo pakeitimai, susiję su išorėje kuriamomis kodų bazėmis, prieš įgyvendinimą būtų peržiūrėti ir patvirtinti.

10.1.3 P13 - Duomenų klasifikavimo ir ženklinimo politika: nustato, kaip jautrūs duomenys turi būti identifikuojami prieš juos atskleidžiant kūrimo tiekėjams ar saugykloms.

10.1.4 P18 - Kriptografinių kontrolės priemonių politika: nustato, kaip kūrimo ir perdavimo metu turi būti tvarkomi raktai, paslaptys ir jautrūs prisijungimo duomenys.

10.1.5 P24 - Saugaus kūrimo politika: nustato bazinius reikalavimus vidinėms ir išorinėms programinės įrangos kūrimo praktikoms.

10.1.6 P30 - Reagavimo į incidentus politika: reglamentuoja, kaip su išoriniu kūrimu susiję pažeidimai ar saugumo klausimai turi būti eskaluojami, tiriami ir sprendžiami.

10.1.7 P33 - Audito ir atitikties stebėsenos politika: nustato reikalavimus išorinio kūrimo veiklų peržiūrai auditų ar atitikties peržiūrų metu.

11. Pamatiniai standartai ir sistemos

11.1 Ši politika suderinta su tarptautiniu mastu pripažintomis saugumo sistemomis ir reglamentais, siekiant užtikrinti saugų programinės įrangos kūrimo perdavimą išorei ir tiekėjų valdymo praktiką.

11.2 ISO/IEC 27001

11.2.1 8.1 skyrius – Veiklos planavimas ir kontrolė: nustato procesų kontrolės priemones saugiam kūrimui ir trečiųjų šalių rezultatų teikimui.

11.3 ISO/IEC 27002:2022 – kontrolės priemonės 5.19–5.21, 8

11.3.1 A priedo kontrolės priemonė 5.19 – Tiekėjų santykių valdymas: reikalauja formalių susitarimų su saugumo ir atitikties nuostatomis.

11.3.2 A priedo kontrolės priemonė 5.20 – Informacijos saugumo užtikrinimas tiekėjų susitarimuose: užtikrina, kad su kūrimu susijusios kontrolės priemonės būtų integruotos į sutartis.

11.3.3 A priedo kontrolės priemonė 5.21 – Tiekėjų paslaugų teikimo valdymas: apima trečiųjų šalių kūrimo rezultatų ir rizikų stebėseną.

11.3.4 A priedo kontrolės priemonė 8.27 – Išorinis kūrimas: nustato apibrėžtus saugumo reikalavimus ir prieigos kontrolę išorėje kuriamai programinei įrangai.

11.3.5 Šios kontrolės priemonės nustato struktūruotus reikalavimus išorės programuotojų atrankai, sutarčių sudarymui ir priežiūrai, įskaitant saugaus kūrimo praktikas, kodo tvarkymą ir veiksmingumo validavimą.

11.4 NIST SP 800-53 Rev.

11.4.1 SA-4 – Įsigijimo procesas: reikalauja saugaus kūrimo reikalavimus apibrėžti įsigijimo etape.

11.4.2 SA-9 – Išorinių sistemų paslaugos: reglamentuoja, kaip trečiųjų šalių programuotojai turi saugiai sąveikauti su vidinėmis paslaugomis.

11.4.3 SA-10 – Kūrėjo konfigūracijos valdymas: atitinka versijų kontrolės, prieigos prie kodo ir pakeitimų sekimo reikalavimus, taikomus išorės komandoms.

11.5 ES BDAR (2016/679)

11.5.1 28 straipsnis – Duomenų tvarkytojo pareigos: reikalauja, kad sutartyse su trečiųjų šalių programuotojais būtų nustatyti saugumo, kontrolės ir audito reikalavimai tvarkant asmens duomenis.

11.5.2 32 straipsnis – Tvarkymo saugumas: reikalauja taikyti tinkamas apsaugos priemones (pvz., šifravimą, prieigos kontrolę) kuriant sistemas, kurios tvarko asmens duomenis.

11.6 ES NIS2 direktyva (2022/2555)

11.6.1 21(2)(a), (h), 23 straipsniai: reikalauja taikyti saugaus kūrimo praktikas visiems trečiųjų šalių bendradarbiavimo atvejams ir skaitmeninėms tiekimo grandinėms, užtikrinant priežiūrą ir techninį patvirtinimą.

11.7 ES DORA reglamentas (2022/2554)

11.7.1 28(1), (2) straipsniai: reikalauja, kad finansų subjektai valdytų IRT trečiųjų šalių riziką taikydami sutartines kontrolės priemones ir saugaus kūrimo priežiūrą, ypač kritinio išorinio kūrimo atvejais.

11.8 COBIT 2019

11.8.1 APO10 – Tiekėjų valdymas: nustato struktūruotus reikalavimus tiekėjų vertinimui, sutartims ir veiksmingumo stebėsenai.

11.8.2 BAI03 – Sprendimų kūrimo valdymas: tiesiogiai siejasi su saugaus SDLC procesais, kodo peržiūromis ir kūrimo validavimu.

11.8.3 DSS05 – Saugumo paslaugų valdymas: atitinka išorėje arba trečiųjų šalių sukurtų sistemų stebėseną ir apsaugą.