| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Čia įrašykite registruoto juridinio asmens pavadinimą | | | | | | | |
| Dokumento numeris:<br>P28S | | | | | Dokumento pavadinimas:<br>**Išorės plėtros politika** | | | | | | | |
| Versija:<br>1.0 | | Įsigaliojimo data:<br>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 | 5.1, 6.1, 8 skyriai | Taikomi informacijos saugumo valdymo sistemos ir su tiekėjais susijusių kontrolės priemonių reikalavimai |
| ISO/IEC 27002:2022 | 5.19, 5.20, 8.25–8.27 kontrolės priemonės | Tiekėjų valdymo ir saugaus kūrimo gyvavimo ciklo kontrolės priemonės |
| NIST SP 800-53 Rev. 5 | SA-4, SA-9, SA-11, SA-15, SR-3 | Įsigijimo, tiekimo grandinės, saugaus kūrimo ir susitarimų su tiekėjais reikalavimai |
| ES BDAR | 28 straipsnis | Sutartiniai ir duomenų apsaugos reikalavimai trečiųjų šalių atliekamam duomenų tvarkymui |
| ES NIS2 direktyva | 21 straipsnio 2 dalies a, h punktai | Tiekimo grandinės saugumo ir saugaus taikomųjų programų kūrimo kontrolės priemonės |
| ES DORA reglamentas | 10 straipsnis | IRT trečiųjų šalių rizikos valdymas, įskaitant išorės plėtrą |
| COBIT 2019 | BAI03, DSS05 | Išorės plėtros ir išorės IT paslaugų teikėjų valdymo reikalavimai |

**1. Tikslas**

1.1 Ši politika užtikrina, kad visa išorės programinės įrangos plėtra, vykdoma laisvai samdomų specialistų, agentūrų ar trečiųjų šalių paslaugų teikėjų, būtų atliekama saugiai, valdoma sutartiniais įsipareigojimais ir atitiktų taikomus teisinius, reguliavimo ir audito reikalavimus.

1.2 Ji apsaugo organizaciją nuo rizikų, susijusių su nesaugiu kodu, neaiškia nuosavybe, duomenų atskleidimu ir netinkamu tiekėjų valdymu, nustatydama privalomus kūrimo standartus ir tiekėjų priežiūrą, net ir nesant atskiro IT padalinio.

1.3 Ši politika padeda užtikrinti ISO/IEC 27001:2022 sertifikavimo reikalavimų laikymąsi, nustatydama aiškius kūrimo reikalavimus, atskaitomybę ir dokumentuotas kontrolės priemones, taikomas trečiųjų šalių vykdomai plėtrai.

**2. Taikymo sritis**

**2.1 Ši politika taikoma:**

2.1.1 Visiems išorės kūrėjams, įskaitant laisvai samdomus specialistus ir plėtros agentūras.

2.1.2 Bet kokiai plėtros veiklai, susijusiai su vidinėmis priemonėmis, viešai pasiekiamomis interneto svetainėmis, programinės įrangos taikomosiomis programomis ar verslo procesų automatizavimu.

2.1.3 Darbuotojams, atsakingiems už išorės kūrėjų atranką, valdymą ar priežiūrą.

2.1.4 Bet kokiam trečiųjų šalių atliekamam sistemų integravimui, scenarijų kūrimui ar plėtrai, sąveikaujančiai su įmonės duomenimis ar sistemomis.

2.2 Ji taip pat apima bet kurią šalį ar platformą, turinčią prieigą prie įmonės prisijungimo duomenų, duomenų saugyklų, išeitinio kodo saugyklų, testavimo aplinkų ar gamybinės aplinkos sistemų.

**3. Tikslai**

3.1 Užtikrinti, kad visa išorės plėtra atitiktų saugaus programavimo praktiką ir kad kūrėjai būtų sutartiniais įsipareigojimais įpareigoti laikytis dokumentuotų standartų bei konfidencialumo reikalavimų.

3.2 Nustatyti visų rezultatų — kodo, turto, prisijungimo duomenų ir dokumentacijos — nuosavybę, užtikrinant visišką teisių perdavimą įmonei ir atsekamą perdavimą projekto pabaigoje.

3.3 Užkirsti kelią dažniausioms plėtros rizikoms, įskaitant pakartotinį nuosavybinio kodo naudojimą, tiekimo grandinės atakas per bibliotekas, nepalaikomų karkasų naudojimą ir nepatvirtintą administratoriaus lygmens prieigą.

3.4 Reikalauti, kad prieš pradedant kiekvieną išorės projektą būtų parengta dokumentacija, įskaitant sutartis, konfidencialumo susitarimus ir minimalius saugumo reikalavimus.

3.5 Apsaugoti klientų duomenis, sistemas ir vidinius procesus, taikant tinkamą plėtros priežiūrą, testavimą po pristatymo ir saugų sistemų prieigos valdymą.

**4. Vaidmenys ir atsakomybės**

**4.1 Generalinis vadovas (GM)**

4.1.1 Tvirtina visus santykius su tiekėjais ir pasirašo plėtros sutartis.

4.1.2 Užtikrina, kad visa išorės plėtra atitiktų šią politiką.

4.1.3 Pasibaigus projektui panaikina prieigą prie įmonės sistemų.

4.1.4 Peržiūri po pristatymo pateiktą dokumentaciją ir rezultatus.

**4.2 Projekto savininkas (paprastai vidinis darbuotojas arba paskirtas koordinatorius)**

4.2.1 Koordinuoja kasdienį darbą su išorės kūrėju.

4.2.2 Patikrina, ar funkciniai reikalavimai įgyvendinti ir ar rezultatai ištestuoti.

4.2.3 Užtikrina saugų kodo ir prisijungimo duomenų perdavimą.

4.2.4 Informuoja GM apie visas su plėtra susijusias problemas ar incidentus.

[ ... 4.3–8 skyriai nėra įtraukti į šią peržiūrą. Įsigykite visą dokumentą, kad pasiektumėte visą turinį. ... ]

**9. Peržiūros ir atnaujinimo reikalavimai**

**9.1 Metinė peržiūra**

**9.1.1 Šią politiką GM turi peržiūrėti bent kartą per metus. Peržiūra turi užtikrinti, kad politika ir toliau atitiktų:**

9.1.1.1 ISO/IEC 27001 sertifikavimo reikalavimus.

9.1.1.2 Teisinių įpareigojimų pokyčius (pvz., ES BDAR 28 straipsnį, DORA 10 straipsnį).

9.1.1.3 Esamą MVĮ lygmens plėtros praktiką ir trečiųjų šalių rizikas.

**9.2 Tarpinės peržiūros**

**9.2.1 Politikos peržiūros taip pat turi būti atliekamos, kai:**

9.2.1.1 Pasitelkiamas naujas išorės plėtros tiekėjas arba naudojama nauja platforma.

9.2.1.2 Įvyksta reikšmingas incidentas, susijęs su išorės plėtra.

9.2.1.3 Iš esmės pasikeičia naudojamos priemonės, platformos ar aplinkos.

**9.3 Peržiūros procesas**

**9.3.1 GM yra atsakingas už:**

9.3.1.1 Patikrinimą, kad sutartys, konfidencialumo susitarimai ir prieigos kontrolės procesai išliktų veiksmingi.

9.3.1.2 Patvirtinimą, kad esami tiekėjai ir laisvai samdomi specialistai atitinka politikos reikalavimus.

9.3.1.3 Nuostatų peržiūrą, atsižvelgiant į ankstesnių projektų ar incidentų grįžtamąjį ryšį.

**9.4 Versijų kontrolė ir komunikacija**

**9.4.1 Visi pakeitimai turi būti:**

9.4.1.1 Užregistruoti nurodant datą, priežastį ir pakeitimo aprašymą.

9.4.1.2 Patvirtinti GM ir įtraukti į versijų istoriją.

9.4.1.3 Komunikuoti visiems darbuotojams ar projektų savininkams, dirbantiems su išorės kūrėjais.

9.4.1.4 Prireikus pakartotinai išplatinti visiems susijusiems tiekėjams ir trečiosioms šalims.

## 10. Susijusios politikos ir sąsajos

**10.1 Ši politika tiesiogiai palaiko toliau nurodytų MVĮ pritaikytų politikų įgyvendinimą ir yra su jomis susijusi:**

10.1.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: paaiškina, kas atsakingas už tiekėjų tvirtinimą, prieigos kontrolę ir rizikos prisiėmimą, kai pasitelkiami išorės kūrėjai.

10.1.2 P4S – Prieigos kontrolės politika: apibrėžia tinkamą naudotojų paskyrų ir administratoriaus lygmens prieigos, naudojamos išorės plėtros metu, sukūrimą, apribojimą ir panaikinimą.

10.1.3 P8S – Informacijos saugumo supratimo didinimo ir mokymo politika: užtikrina, kad vidaus darbuotojai suprastų, kaip saugiai koordinuoti darbą su išorės kūrėjais, įskaitant prisijungimo duomenų ir projekto failų tvarkymą.

10.1.4 P17S – Duomenų apsaugos ir privatumo politika: nustato saugumo ir teisinius reikalavimus asmens duomenų, kuriuos pagal ES BDAR gali tvarkyti ar pasiekti išorės kūrėjai, tvarkymui.

10.1.5 P24S – Saugaus kūrimo politika: nustato, kaip vidinė ir išorės plėtra turi atitikti saugaus programavimo praktiką ir bibliotekų bei karkasų patikros reikalavimus.

10.1.6 P30S – Reagavimo į incidentus politika: taikoma, kai dėl išorės plėtros kyla saugumo incidentai ar pažeidžiamumai, ir nustato koordinuoto tyrimo bei taisomųjų veiksmų gaires.

10.2 Šios politikos turi būti įgyvendinamos lygiagrečiai, siekiant užtikrinti, kad išorės plėtra nesukurtų nevaldomos rizikos ir nepažeistų MVĮ atitikties įpareigojimų.

## 11. Pamatiniai standartai ir sistemos

**11.1 ISO/IEC 27001**

11.1.1 6.1 skyrius – Organizacijos privalo vertinti ir tvarkyti su tiekėjais susijusias informacijos saugumo rizikas.

11.1.2 8.1 skyrius – Reikalaujama operacinio planavimo ir kontrolės, įskaitant trečiųjų šalių paslaugas, tokias kaip išorės plėtra.

**11.2 ISO/IEC 27002**

11.2.1 5.19 kontrolės priemonė – Rekomenduojama vertinti tiekėjų gebėjimą atitikti informacijos saugumo reikalavimus.

11.2.2 5.20 kontrolės priemonė – Rekomenduojama reguliariai stebėti trečiųjų šalių paslaugas ir periodiškai jas peržiūrėti.

11.2.3 8.25–8.27 kontrolės priemonės – Apibrėžia saugaus kūrimo gyvavimo ciklo praktiką, taikytiną išorės plėtrai.

**11.3 NIST SP 800-53 Rev. 5**

11.3.1 SA-4 – Reikalaujama, kad įsigijimo strategijos apimtų informacijos saugumo priemones.

11.3.2 SA-9 – Apima išorinių sistemų kūrimą ir tiekimo grandinės rizikas.

11.3.3 SA-11 – Apibrėžia saugaus kūrimo praktiką, įskaitant kodo peržiūras ir trūkumų šalinimą.

11.3.4 SA-15 – Rekomenduojama naudoti automatizuotas priemones trūkumams aptikti ir programinės įrangos patikimumui užtikrinti.

11.3.5 SR-3 – Nustatoma, kad susitarimuose su tiekėjais turi būti įtraukti kibernetinio saugumo reikalavimai.

**11.4 Europos Sąjungos bendrasis duomenų apsaugos reglamentas (BDAR)**

11.4.1 28 straipsnis – Reikalaujama, kad sutartys su trečiųjų šalių duomenų tvarkytojais užtikrintų tinkamas duomenų apsaugos priemones; tai tiesiogiai taikoma kūrėjams, tvarkantiems ar turintiems prieigą prie asmens duomenų.

**11.5 ES NIS2 direktyva (2022/2555)**

11.5.1 21 straipsnio 2 dalies a, h punktai – Reikalaujama taikyti tiekimo grandinės saugumo kontrolės priemones ir saugaus programinės įrangos kūrimo praktiką į taikymo sritį patenkantiems skaitmeninių paslaugų teikėjams, įskaitant MVĮ, kai taikoma.

**11.6 ES Skaitmeninio operacinio atsparumo aktas (DORA)**

11.6.1 10 straipsnis – Reikalaujama valdyti IRT trečiųjų šalių riziką, įskaitant plėtros susitarimus, saugumo įpareigojimus ir rizikos kontrolės priemones, susijusias su trečiųjų šalių paslaugų teikėjais.

**11.7 COBIT 2019**

11.7.1 BAI03 – Sprendimų identifikavimo ir kūrimo valdymas – užtikrina, kad išorės plėtra atitiktų verslo reikalavimus ir saugumo lūkesčius.

11.7.2 DSS05 – Saugumo paslaugų valdymas – reikalaujama, kad išorės saugumo paslaugos ir plėtros paslaugų teikėjai veiktų pagal taikomas saugumo taisykles ir priežiūros reikalavimus.