					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: P25S					Dokumento pavadinimas: **Taikomųjų programų saugumo reikalavimų 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 skyrius	Veiklos kontrolės priemonės, įskaitant taikomųjų programų saugumą
ISO/IEC 27002:2022	Kontrolės priemonės 8.25–8.26	Saugus projektavimas, kūrimas, testavimas ir kodo peržiūra
NIST SP 800-53 Rev.5	SA-11, SI-10	Kūrėjų ir taikomųjų programų testavimas, kodo analizė, trūkumų prevencija
ES BDAR	25 straipsnis	Duomenų apsauga pagal projektavimą ir numatytuosius nustatymus
ES NIS2 direktyva	21 straipsnio 2 dalies a, e punktai	Techninės priemonės taikomosioms programoms apsaugoti ir rizikoms aptikti
ES DORA reglamentas	9 straipsnio 2 dalies c punktas, 10 straipsnio 2 dalies c punktas	Taikomųjų programų saugumas skaitmeniniam veiklos atsparumui užtikrinti
COBIT 2019	BAI03	Saugaus programinės įrangos kūrimo ir įsigijimo valdymas

1. Tikslas

1.1 Ši politika nustato minimalius privalomus taikomųjų programų saugumo kontrolės priemonių reikalavimus, taikomus visai organizacijos naudojamai programinei įrangai ir sisteminiams sprendimams, nepriklausomai nuo to, ar jie sukurti organizacijos viduje, ar įsigyti iš išorės tiekėjų.

1.2 Ji užtikrina, kad taikomosios programos būtų projektuojamos, įgyvendinamos ir prižiūrimos taip, kad klientų, darbuotojų ir veiklos duomenys būtų apsaugoti nuo neteisėtos prieigos, netinkamo naudojimo, pakeitimo ar sunaikinimo.

1.3 Ši politika padeda organizacijai siekti ir palaikyti ISO/IEC 27001 sertifikavimą, vykdyti ES BDAR ir NIS2 direktyvos reikalavimus bei mažinti veiklos riziką, susijusią su nesaugios programinės įrangos diegimu.

1.4 Ji padeda užtikrinti nuoseklų ir audituojamą požiūrį į taikomųjų programų saugumą MVĮ aplinkoje, nustatydama vieningą saugumo funkcijų ir praktikų kontrolinį sąrašą, pritaikytą aplinkoms, kuriose vidaus techniniai ištekliai yra riboti.

2. Taikymo sritis

2.1 Ši politika taikoma visoms taikomosioms programoms, sistemoms, priemonėms ir platformoms, kurios:

2.1.1 kuriamos organizacijos viduje, pritaikomos arba skriptinamos vidaus naudojimui;

2.1.2 įsigyjamos kaip komercinė programinė įranga, SaaS paslaugos arba debesijos aplinkoje veikiančios sistemos;

2.1.3 tvarko, saugo arba perduoda asmens duomenis, veiklos įrašus ar jautrią veiklos informaciją;

2.1.4 yra prieinamos darbuotojams, rangovams, klientams ar partneriams per vidinius tinklus, internetą ar mobiliąsias platformas.

2.2 Politika taikoma:

2.2.1 kūrėjams (vidiniams arba samdomiems);

2.2.2 programinės įrangos tiekėjams ir debesijos paslaugų teikėjams;

2.2.3 IT pagalbos darbuotojams arba administratoriams, atsakingiems už diegimą ir palaikymą;

2.2.4 taikomųjų programų savininkams ir veiklos naudotojams, dalyvaujantiems sistemų tvirtinime ir priežiūroje.

3. Tikslai

3.1 Užtikrinti, kad visose organizacijos naudojamose taikomosiose programose būtų įdiegtos ir patikrinamos saugumo kontrolės priemonės, mažinančios dažniausiai pasitaikančius programinės įrangos pažeidžiamumus.

3.2 Apsaugoti taikomųjų programų tvarkomų duomenų konfidencialumą, vientisumą ir prieinamumą, nepriklausomai nuo jų talpinimo vietos.

3.3 Nustatyti privalomą formalų taikomųjų programų saugumo testavimą, peržiūrą ir validavimą prieš patvirtinant bet kurią naują taikomąją programą ar esminį atnaujinimą naudoti gamybinėje aplinkoje.

3.4 Užtikrinti nuoseklų ir saugų naudotojų prisijungimo duomenų, sesijų duomenų ir prieigos teisių tvarkymą visose veiklai kritinėse sistemose.

3.5 Nustatyti reikalavimą, kad visose taikomosiose programose būtų įdiegtos saugaus žurnalų tvarkymo, audituojamumo ir stebėsenos funkcijos, padedančios aptikti įtartiną veiklą ir į ją reaguoti.

3.6 Mažinti teisines ir atitikties rizikas užtikrinant, kad taikomosios programos atitiktų taikomus reguliavimo saugumo reikalavimus.

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas (GM)

4.1.1 Atsako už bendrą taikomųjų programų saugumą visoje organizacijoje.

4.1.2 Tvirtina šią politiką ir užtikrina, kad visi įsigijimo ar kūrimo projektai jos laikytųsi.

4.1.3 Užtikrina, kad sutartyse su tiekėjais ir paslaugų teikėjais būtų nustatyti taikomųjų programų saugumo reikalavimai.

4.1.4 Peržiūri ir tvirtina rizikos išimtis tais atvejais, kai dėl veiklos apribojimų neįmanoma pasiekti visiškos atitikties.

4.2 Taikomosios programos savininkas (jei paskirtas)

4.2.1 Nustato konkrečiai taikomajai programai taikomus saugumo poreikius sistemos pasirinkimo arba projekto inicijavimo metu.

4.2.2 Patikrina, ar įdiegtos pagrindinės funkcijos, tokios kaip prisijungimo apsauga, šifravimas ir veiksmų registravimas audito žurnaluose.

4.2.3 Dalyvauja peržiūrose prieš diegimą ir patvirtina, kad saugumo kontrolės priemonės atitinka veiklos poreikius.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Šią politiką Generalinis vadovas privalo peržiūrėti bent kartą per kalendorinius metus, siekdamas:

9.1.1 atspindėti reguliavimo reikalavimų pokyčius (pvz., ES BDAR, NIS2 direktyvos, DORA reglamento);

9.1.2 įtraukti naujas ar kylančias grėsmes ir atakų metodus;

9.1.3 atnaujinti formuluotes ir reikalavimus, atsižvelgiant į platformų, tiekėjų ar kūrimo metodų pokyčius.

9.2 Tarpinės peržiūros taip pat turi būti atliekamos, kai:

9.2.1 diegiamos naujos taikomosios programos;

9.2.2 esamoms taikomosioms programoms atliekami reikšmingi atnaujinimai ar integracija;

9.2.3 įvyksta su taikomąja programa susijęs incidentas ar duomenų saugumo pažeidimas;

9.2.4 naujos rizikos nustatomos pagal išorės pranešimus ar pramonės įspėjimus.

9.3 Visi šios politikos atnaujinimai turi būti:

9.3.1 patvirtinti Generalinio vadovo;

9.3.2 dokumentuoti nurodant versijų istoriją ir pakeitimo priežastį;

9.3.3 komunikuojami visiems darbuotojams, kūrėjams ir tiekėjams, dalyvaujantiems taikomųjų programų valdyme;

9.3.4 saugiai saugomi audito ir atitikties tikslais.

10. Susijusios politikos ir sąsajos

10.1 Šią politiką tiesiogiai papildo ir jos taikymą užtikrina šios su MVĮ suderintos saugumo politikos:

10.1.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: nustato atsakomybę už taikomųjų programų tvirtinimą, politikos taikymą ir tiekėjų valdymą.

10.1.2 P4S – Prieigos kontrolės politika: užtikrina, kad prieiga prie taikomųjų programų atitiktų mažiausių privilegijų principą ir sesijų kontrolės reikalavimus.

10.1.3 P8S – Informacijos saugumo supratimo didinimo ir mokymų politika: užtikrina, kad naudotojai ir kūrėjai būtų apmokyti atpažinti ir pranešti apie su taikomosiomis programomis susijusias grėsmes.

10.1.4 P17S – Duomenų apsaugos ir privatumo politika: nustato duomenų privatumo apsaugos priemones, kurios turi būti taikomos bet kurioje taikomojoje programoje, tvarkančioje asmens duomenis.

10.1.5 P14S – Duomenų saugojimo ir sunaikinimo politika: reglamentuoja, kaip turi būti saugomi, archyvuojami ir saugiai sunaikinami taikomųjų programų generuojami žurnalai, atsarginės kopijos ir jautrūs duomenys.

10.1.6 P30S – Reagavimo į incidentus politika: nustato veiksmus, skirtus taikomųjų programų saugumo įvykiams nustatyti, apie juos pranešti ir juos lokalizuoti.

10.2 Kartu šios politikos užtikrina, kad taikomųjų programų saugumas būtų visiškai integruotas į organizacijos informacijos saugumo valdymo sistemą (ISVS) ir būtų užtikrintas pasirengimas auditui.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8.1 punktas – reikalauja, kad organizacijos nustatytų veiklos kontrolės priemones informacijos saugumo rizikoms valdyti, įskaitant rizikas, susijusias su taikomosiomis programomis ir programinės įrangos sistemomis.

11.2 ISO/IEC 27002

11.2.1 Kontrolės priemonė 8.25 – rekomenduoja visose taikomosiose programose, įskaitant tiekėjų pateiktas, taikyti saugaus projektavimo, kūrimo ir kodo peržiūros praktikas.

11.2.2 Kontrolės priemonė 8.26 – rekomenduoja formalų taikomųjų programų saugumo kontrolės priemonių testavimą, ypač prieigos kontrolės, įvesties tikrinimo ir sesijų valdymo srityse.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – nustato reikalavimus kūrėjų testavimui, kodo analizei ir dinaminiam taikomųjų programų skenavimui prieš diegimą.

11.3.2 SI-10 – apima dažniausiai pasitaikančių programinės įrangos trūkumų aptikimą ir prevenciją, pabrėžiant kūrėjų informuotumą ir technines apsaugos priemones.

11.4 ES BDAR (2016/679)

11.4.1 25 straipsnis – „duomenų apsauga pagal projektavimą ir numatytuosius nustatymus“ reikalauja privatumo ir saugumo priemones integruoti į pagrindinį asmens duomenis tvarkančių taikomųjų programų projektą.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21 straipsnio 2 dalies a ir e punktai – reikalauja, kad esminiai ir svarbūs subjektai įgyvendintų technines priemones taikomosioms programoms apsaugoti ir su programine įranga susijusioms rizikoms aptikti.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 9 straipsnio 2 dalies c punktas, 10 straipsnio 2 dalies c punktas – reikalauja, kad finansų sektoriaus MVĮ įdiegtų taikomųjų programų lygmens saugumo kontrolės priemones ir reguliariai atliktų vertinimus skaitmeniniam veiklos atsparumui palaikyti.

11.7 COBIT 2019

11.7.1 BAI03 – „sprendimų identifikavimo ir kūrimo valdymas“ pateikia gaires, kaip kurti arba įsigyti saugią programinę įrangą, suderintą su rizikos, atitikties ir veiklos reikalavimais, net ir ribotų išteklių MVĮ aplinkoje.