					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: P25					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	Skyrius / straipsnis	Komentaras
ISO/IEC 27001:2022	8 skyrius	—
ISO/IEC 27002:2022	Kontrolės priemonės 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
ES BDAR	25, 32 straipsniai	—
ES NIS2 direktyva	21(2)(f), 23 straipsniai	—
ES DORA reglamentas	9, 11 straipsniai	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Tikslas

1.1 Ši politika nustato privalomuosius taikomųjų programų saugumo reikalavimus programinei įrangai, kurią organizacija kuria, įsigyja, integruoja arba diegia. Ji užtikrina, kad visos taikomosios programos būtų projektuojamos, įgyvendinamos ir prižiūrimos laikantis saugaus kūrimo principų, reguliavimo reikalavimų ir organizacijos rizikos apetito.

1.2 Ši politika nustato privalomus saugumo užtikrinimo reikalavimus visam taikomosios programos gyvavimo ciklui, apimant naudotojų autentifikavimą, duomenų tvarkymą, sąsajų apsaugą ir saugią sąveiką su taikomųjų programų sąsajomis ir paslaugomis.

1.3 Taikydama šią politiką, organizacija siekia užkirsti kelią programinės įrangos pažeidžiamumų atsiradimui, apsaugoti jautrius duomenis ir užtikrinti atsekamumą bei atsparumą išnaudojimui ir piktnaudžiavimui.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 Organizacijos viduje sukurtoms arba iš išorės įsigytoms taikomosioms programoms, įskaitant SaaS sprendimus ir pagal užsakymą sukurtus įrankius

2.1.2 Taikomosioms programoms, kurios palaiko kritines verslo operacijas, klientų prieigą arba tvarko reglamentuojamus duomenis

2.1.3 Kūrimo, „DevOps“, kokybės užtikrinimo, produktų ir saugumo komandoms

2.1.4 Trečiųjų šalių programuotojams, programinės įrangos tiekėjams ir integravimo partneriams, turintiems prieigą prie organizacijos taikomųjų programų arba taikomųjų programų programavimo sąsajų

2.2 Ji taikoma visose aplinkose: kūrimo, testavimo, parengiamojoje, gamybinėje ir atkūrimo po katastrofos aplinkoje, nepriklausomai nuo to, ar jos talpinamos vietinėje infrastruktūroje, privačiuose duomenų centruose, ar viešosios debesijos aplinkose.

3. Tikslai

3.1 Nustatyti bazinius funkcinius ir nefunkcinius saugumo reikalavimus, kuriuos turi atitikti visos taikomosios programos, nepriklausomai nuo kūrimo metodo ar technologijų paketo.

3.2 Užtikrinti taikomojo lygmens apsaugos priemonių integravimą, įskaitant įvesties validavimą, išvesties kodavimą, klaidų tvarkymą ir sesijų saugumą.

3.3 Nustatyti privalomą saugų autentifikavimo, autorizavimo ir prieigos kontrolės mechanizmų įgyvendinimą, suderintą su organizacijos tapatybių ir prieigos valdymo politikomis.

3.4 Nustatyti privalomą saugią sąveiką su programavimo sąsajomis, žiniatinklio sąsajomis ir trečiųjų šalių komponentais, naudojant patvirtintą aparatinę įrangą, protokolus ir saugos kontrolės priemones.

3.5 Sudaryti sąlygas anksti aptikti pažeidžiamumus ir mažinti jų riziką taikant statinę ir dinaminę analizę, kodo peržiūras ir grėsmių modeliavimą.

3.6 Apsaugoti jautrius duomenis laikantis reguliavimo reikalavimų, užtikrinant šifravimą, klasifikavimą ir duomenų saugojimo logiką.

3.7 Užtikrinti nuolatinį taikomųjų programų saugumo būklės tikrinimą po diegimo, taikant testavimą, stebėseną ir pasirengimą auditui.

4. Vaidmenys ir atsakomybės

4.1 Informacijos saugumo vadovas (CISO)

4.1.1 Valdo šią politiką ir užtikrina jos suderinamumą su organizacijos informacijos saugumo strategija ir rizikos laikysena.

4.1.2 Tvirtina taikomųjų programų saugumo reikalavimus ir užtikrina privalomų kontrolės priemonių taikymą kūrimo ir pirkimų funkcijose.

4.2 Taikomųjų programų saugumo vadovas / „DevSecOps“ vadovas

4.2.1 Nustato bazines saugumo kontrolės priemones ir taikomųjų programų komponentų testavimo metodikas.

4.2.2 Prižiūri saugią priemonių, tokių kaip SAST, DAST, IAST ir SCA, integraciją į programinės įrangos teikimo grandinę.

4.2.3 Prižiūri taikomųjų programų saugumo reikalavimų kontrolinį sąrašą ir validavimo kriterijus.

[... 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 Kritinių pažeidžiamumų atskleidimai, darantys poveikį plačiai naudojamoms sistemoms ar priklausomybėms

9.1.2 Reguliavimo reikalavimų, susijusių su taikomųjų programų saugumu, atnaujinimai, pvz., NIS2 direktyva arba DORA reglamentas

9.1.3 Esminiai organizacijos programinės įrangos kūrimo praktikos, priemonių ar debesijos architektūros pokyčiai

9.1.4 Vidaus auditų arba išorinių įsiskverbimo testų išvados

9.2 Peržiūrai turi vadovauti taikomųjų programų saugumo vadovas, koordinuodamas veiksmus su informacijos saugumo vadovu (CISO), „DevOps“ inžinerijos, teisinės funkcijos, pirkimų ir kokybės užtikrinimo vadovais.

9.3 Visi pakeitimai turi būti valdomi taikant versijų kontrolę ISVS dokumentų registre ir išplatinti visoms susijusioms kūrimo ir produktų komandoms.

9.4 Pakeistos versijos turi būti archyvuojamos ne trumpiau kaip trejus metus, siekiant užtikrinti atsekamumą, audituojamumą ir paramą duomenų saugumo pažeidimų tyrimams.

10. Susijusios politikos ir sąsajos

10.1 P1 – Informacijos saugumo politika. Nustato sistemų ir duomenų apsaugos pagrindą, pagal kurį taikomojo lygmens kontrolės priemonės yra būtinos siekiant užkirsti kelią neteisėtai prieigai, duomenų nutekėjimui ir išnaudojimui.

10.2 P4 – Prieigos kontrolės politika. Nustato tapatybių ir sesijų valdymo standartus, kurių turi laikytis visos taikomosios programos, įskaitant stiprų autentifikavimą, mažiausių privilegijų principą ir prieigos peržiūrų reikalavimus.

10.3 P5 – Pakeitimų valdymo politika. Reglamentuoja taikomųjų programų kodo ir konfigūracijų perkėlimą į gamybines aplinkas, užtikrinant, kad nesankcionuoti arba neištestuoti pakeitimai būtų blokuojami.

10.4 P17 – Duomenų apsaugos ir privatumo politika. Reikalauja, kad taikomosios programos įgyvendintų privatumo užtikrinimą pagal projektavimą ir užtikrintų teisėtą asmens ir jautrių duomenų tvarkymą, šifravimą bei saugojimą visose aplinkose.

10.5 P24 – Saugaus kūrimo politika. Pateikia platesnę sistemą saugumui integruoti į SDLC, o ši politika nustato konkrečius reikalavimus ir technines apsaugos priemones, kurios turi būti įgyvendintos taikomojo lygmens srityje.

10.6 P30 – Reagavimo į incidentus politika. Nustato struktūruotą taikomųjų programų saugumo incidentų tvarkymą, įskaitant po diegimo arba įsiskverbimo testavimo metu nustatytus pažeidžiamumus, ir apibrėžia eskalavimo, lokalizavimo ir atkūrimo procedūras.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001:2022

11.1.1 8.1 skyrius – Operacijų planavimas ir kontrolė: reikalauja, kad taikomųjų programų saugumas būtų integruotas į procesus ir sistemas, siekiant užtikrinti konfidencialumą, vientisumą ir prieinamumą.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrolės priemonės 8.25–8.26: detalizuoja taikomojo lygmens saugumo lūkesčius, įskaitant saugaus programavimo praktiką, grėsmių modeliavimą, architektūrines kontrolės priemones ir trečiųjų šalių programinės įrangos validavimą.

11.2.2 A priedo kontrolės priemonė 8.25 – Saugus kūrimo gyvavimo ciklas: nustato privalomą saugumo integravimą per visą taikomosios programos gyvavimo ciklą.

11.2.3 A priedo kontrolės priemonė 8.26 – Taikomųjų programų saugumo reikalavimai: nustato privalomą techninių kontrolės priemonių apibrėžimą ir taikymą, siekiant apsaugoti taikomąsias programas nuo netinkamo naudojimo ir kompromitavimo.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Kūrėjo atliekamas saugumo testavimas ir vertinimas: nustato privalomą statinį, dinaminį ir įsiskverbimo testavimą kūrimo metu.

11.3.2 SA-15 – Kūrimo procesai, standartai ir priemonės: nustato formalius saugaus taikomųjų programų kūrimo standartus.

11.3.3 SI-10 – Informacijos įvesties tikrinimas: reikalauja kontrolės mechanizmų, skirtų užkirsti kelią įterpimo ir analizavimo atakoms.

11.4 ES BDAR (2016/679)

11.4.1 25 straipsnis – Duomenų apsauga pagal projektavimą ir pagal numatytuosius nustatymus: reikalauja duomenų apsaugą ir privatumą integruoti į taikomųjų programų logiką ir darbo eigą.

11.4.2 32 straipsnis – Tvarkymo saugumas: nustato tinkamas technines priemones, tokias kaip įvesties tikrinimas, šifravimas ir saugios prieigos kontrolės priemonės.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21(2)(f) straipsnis: reikalauja pažeidžiamumų tvarkymo ir saugaus taikomųjų programų gyvavimo ciklo praktikos esminiams ir svarbiems subjektams.

11.5.2 23 straipsnis – Saugumo incidentų pranešimas: reikalauja taikomojo lygmens žurnalų tvarkymo ir stebėsenos galimybių reikšmingiems incidentams aptikti ir apie juos pranešti.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 9 straipsnis – IRT rizikos valdymas: įpareigoja finansų sektoriaus subjektus užtikrinti, kad taikomosios programos būtų saugios, ištestuotos ir atsparios kibernetinėms grėsmėms.

11.6.2 11 straipsnis – IRT priemonių testavimas: skatina periodinį kritinių taikomųjų programų ir paslaugų įsiskverbimo testavimą bei „red team“ pratybas.

11.7 COBIT 2019

11.7.1 BAI03 – Sprendimų identifikavimo ir kūrimo valdymas: nustato projektavimo ir kontrolės reikalavimus taikomųjų programų kūrimo metu.

11.7.2 BAI09 – Taikomųjų programų valdymas: pabrėžia saugią veikiančių taikomųjų programų priežiūrą, stebėseną ir tobulinimą.

11.7.3 DSS05 – Saugumo paslaugų valdymas: susieja taikomųjų programų apsaugą su platesnėmis organizacijos saugumo operacijomis ir kontrolės priemonėmis.