					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P05					Dokumento pavadinimas: **Pakeitimų valdymo 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 reglamentavimo reikalavimais

Standartas / reglamentas	Skyrius / straipsnis	Pastaba
ISO/IEC 27001:2022	6.1, 5 skyriai	Apima veiksmus rizikai valdyti, prieigos kontrolę ir pakeitimų valdymą
ISO/IEC 27002:2022	Kontrolė 8	Įgyvendina struktūrizuotą pakeitimų valdymo procesą
NIST SP 800-53 Rev.5	CM-2–CM-14	Konfigūracijų valdymo kontrolės priemonės
ES BDAR	32 straipsnio 1 dalies b–d punktai, 25 straipsnis; 78 konstatuojamoji dalis	Techninės ir organizacinės priemonės sistemų ir duomenų saugumui užtikrinti vykdant pakeitimus
ES NIS2 direktyva	21 straipsnio 2 dalies a, b, d, e punktai	Nustato IRT pakeitimų rizikos valdymo reikalavimus
ES DORA reglamentas	5, 8, 12 straipsniai	Reglamentuoja operacinę / IRT riziką ir pranešimą apie incidentus
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Struktūrizuotas IT pakeitimų valdymo veiksmingumas, atitiktis ir reikalavimai

1. Tikslas

1.1. Ši politika nustato formalią sistemą organizacijos informacinių sistemų, infrastruktūros, taikomųjų programų ir susijusių procesų pakeitimams inicijuoti, vertinti, tvirtinti, įgyvendinti ir peržiūrėti.

1.2. Ji užtikrina, kad visi pakeitimai būtų vykdomi kontroliuojamai, išlaikant audito pėdsaką ir kiek įmanoma mažinant veiklos sutrikimų, saugumo incidentų ar reglamentavimo reikalavimų neatitikties riziką.

1.3. Ji palaiko ISO/IEC 27001:2022 A priedo kontrolės 8.32 įgyvendinimą, nustatydama saugias, dokumentuotas ir su rizika suderintas pakeitimų valdymo praktikas.

1.4. Politika taip pat užtikrina pakeitimų sprendimų atsekamumą ir stiprina operacinį atsparumą vykdant planinius ar neatidėliotinus pakeitimus.

2. Taikymo sritis

2.1. Ši politika taikoma visiems pakeitimams, darantiems poveikį sistemoms, duomenims ir aplinkoms, patenkančioms į informacijos saugumo valdymo sistemos taikymo sritį, įskaitant:

2.1.1. IT infrastruktūrą (vietinę, debesijos, hibridinę)

2.1.2. Produkcines, priešprodukcines ir atkūrimo po katastrofos aplinkas

2.1.3. Verslo taikomąsias programas, paslaugas, taikomųjų programų sąsajas ir integracijas

2.1.4. Konfigūracijos parametrus, pataisų diegimą, programinės įrangos leidimus ir sistemų migravimą

2.1.5. Neatidėliotinas pataisas ir projektinius arba planinius pakeitimus

2.2. Ji reglamentuoja pakeitimus, kuriuos inicijuoja:

2.2.1. Vidaus darbuotojai (IT operacijų specialistai, programuotojai, sistemų savininkai)

2.2.2. Išoriniai tiekėjai, valdomų paslaugų teikėjai (MSP) ir rangovai

2.2.3. Projektų komandos sistemų diegimo, atnaujinimų ar paslaugų perdavimo metu

2.3. Ši politika netaikoma:

2.3.1. laikinoms testavimo ir kūrimo aplinkoms, neturinčioms prieigos prie produkcinių duomenų

2.3.2. asmeninėms naudotojų konfigūracijoms (reglamentuojama Priimtino naudojimo politika)

2.3.3. pakeitimams sistemose, esančiose už organizacijos kontrolės ribų, nebent jie daro poveikį integruotiems informacijos ištekliams arba atitikties įpareigojimams

3. Tikslai

3.1. Užtikrinti, kad visi pakeitimai prieš įgyvendinimą būtų peržiūrėti, patvirtinti, ištestuoti ir dokumentuoti.

3.2. Išlaikyti sistemų prieinamumą, duomenų vientisumą ir paslaugų tęstinumą pakeitimų vykdymo metu ir po jų.

3.3. Reikalauti apibrėžtų pakeitimų klasifikacijų, grąžinimo į ankstesnę būseną planų ir rizikos vertinimų visų tipų pakeitimams.

3.4. Sudaryti sąlygas skaidriam sprendimų priėmimui ir eskalavimui taikant struktūrizuotą valdyseną.

3.5. Palaikyti pasirengimą auditui, užtikrinant atsekamus pakeitimų įrašus ir poįgyvendinę peržiūrą.

3.6. Užtikrinti pareigų atskyrimą ir mažinti nesankcionuotų ar tarpusavyje konfliktuojančių pakeitimų riziką kritinėse sistemose.

4. Vaidmenys ir atsakomybės

4.1. Aukščiausioji vadovybė

4.1.1. Tvirtina Pakeitimų valdymo politiką ir užtikrina jos suderinamumą su strateginiais tikslais ir reglamentavimo įpareigojimais.

4.1.2. Vykdydama valdysenos priežiūrą, tvirtina didelio poveikio arba tarpfunkcines pakeitimų programas.

4.1.3. Skiria reikiamus išteklius ir biudžetą pakeitimų kontrolės priemonėms ir darbuotojų mokymams.

4.2. Pakeitimų patariamoji taryba

4.2.1. Peržiūri ir tvirtina standartinius ir didelius pakeitimus, užtikrindama tinkamą rizikos, poveikio ir priklausomybių vertinimą.

4.2.2. Patvirtina grąžinimo į ankstesnę būseną planus, testavimo rezultatus, suinteresuotųjų šalių komunikaciją ir planavimą.

4.2.3. Ją sudaro sistemų savininkai, informacijos saugumo, IT operacijų, verslo vadovų ir atitikties atstovai.

4.2.4. Esant dokumentuotoms sąlygoms, gali deleguoti sprendimus dėl mažos rizikos arba neatidėliotinų pakeitimų.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1. Peržiūros inicijavimo sąlygos ir periodiškumas

9.1.1. Ši politika turi būti peržiūrima kasmet arba įvykus:

9.1.1.1. dideliems IT arba infrastruktūros pakeitimams

9.1.1.2. reikšmingiems incidentams, susijusiems su nepavykusiais arba nesankcionuotais pakeitimais

9.1.1.3. reglamentavimo atnaujinimams arba naujiems su pakeitimais susijusiems teisiniams įpareigojimams

9.1.1.4. naujų priemonių arba CMS platformų įdiegimui

9.2. Pakeitimų valdymo politikos peržiūros procesas

9.2.1. Pakeitimų valdymo vadovas vadovauja peržiūros procesui bendradarbiaudamas su:

9.2.1.1. IT, saugumo ir operacijų funkcijomis

9.2.1.2. vidaus audito ir rizikos valdymo funkcijomis

9.2.1.3. Pakeitimų patariamosios tarybos atstovais

9.2.2. Atnaujinimai turi būti peržiūrėti ir patvirtinti Aukščiausiosios vadovybės ir Informacijos saugumo valdymo komiteto.

9.2.3. Pakartotinai išleistos versijos turi būti registruojamos Dokumentų registre ir apie jas turi būti informuojamos paveiktos šalys, prireikus gaunant pakartotinį patvirtinimą.

9.3. Dokumentų kontrolė ir versijų valdymas

9.3.1. Visose versijose turi būti:

9.3.1.1. politikos identifikatorius, pavadinimas ir klasifikavimo lygis

9.3.1.2. savininkas ir peržiūrų istorija

9.3.1.3. pakeitimų žurnalas ir įsigaliojimo data

9.3.1.4. tvirtinanti institucija

9.3.2. Archyvuotos versijos turi būti saugomos pagal Dokumentų saugojimo politiką (ne trumpiau kaip 3 metus).

10. Susijusios politikos ir sąsajos

10.1. Ši politika yra tiesiogiai susijusi su toliau nurodytomis politikomis ir palaiko jų taikymą:

10.1.1. P1 – Informacijos saugos politika: nustato formalių saugumo kontrolės priemonių ir procesų lygmens atskaitomybės reikalavimą, įskaitant pakeitimų valdymo valdyseną.

10.1.2. P2 – Valdysenos vaidmenų ir atsakomybių politika: apibrėžia tvirtinimo įgaliojimus ir pareigų atskyrimą, susijusį su pakeitimų autorizavimu ir priežiūra.

10.1.3. P4 – Prieigos kontrolės politika: užtikrina, kad pakeitimų vykdytojų ir peržiūrėtojų prieigos teisės atitiktų mažiausių privilegijų principą.

10.1.4. P6 – Rizikos valdymo politika: užtikrina, kad visiems pakeitimams būtų taikomas tinkamas rizikos vertinimas ir rizikos mažinimo strategijos.

10.1.5. P33 – Audito ir atitikties stebėsenos politika: reglamentuoja pakeitimų valdymo įrašų ir pažeidimų validavimą bei audito peržiūrą.

10.2. Šios politikos kartu sudaro sąlygas užtikrinamam, atsekamam ir saugiam pakeitimų valdymo gyvavimo ciklui ISVS sistemoje.

11. Pamatiniai standartai ir sistemos

11.1. ISO/IEC 27001:2022

11.1.1. 6.1 skyrius – Veiksmai rizikoms ir galimybėms valdyti: ši politika palaiko su pakeitimais susijusių rizikų identifikavimą, vertinimą ir kontrolę.

11.1.2. 5.15 skyrius – Prieigos kontrolė: užtikrina, kad prieiga vykdant pakeitimus būtų kontroliuojama ir atsekama.

11.1.3. A priedo kontrolė 8.32 – Pakeitimų valdymas: ši politika visiškai įgyvendina reikalavimą planuotai ir kontroliuojamai valdyti informacijos tvarkymo priemonių ir sistemų pakeitimus.

11.2. ISO/IEC 27002:2022 – Kontrolė 8

11.2.1. Sustiprina struktūrizuoto pakeitimų valdymo proceso įgyvendinimą, įskaitant pakeitimų klasifikavimą, tvirtinimą, testavimą, grąžinimą atgal ir dokumentavimą.

11.3. NIST SP 800-53 Rev.5

11.3.1. CM šeima (CM-1–CM-14): ši politika glaudžiai suderinta su konfigūracijų valdymo kontrolės priemonėmis, įskaitant bazines konfigūracijas (CM-2), konfigūracijos pakeitimų kontrolę (CM-3), saugumo poveikio analizę (CM-4) ir prieigos apribojimus (CM-5).

11.3.2. AU šeima (AU-2, AU-6, AU-12): šioje politikoje nurodyti žurnalinimo ir audito mechanizmai palaiko įvykių atsekamumą ir su pakeitimais susijusios veiklos atitikties peržiūrą.

11.3.3. RA-3, RA-5: pakeitimų inicijuojami rizikos vertinimai ir pažeidžiamumų skenavimas yra integruoti į pakeitimų vertinimo procesą.

11.3.4. PM-11 (Misijos / verslo procesų apibrėžimas): užtikrina, kad vykdant pakeitimus būtų išsaugotas veiklos tęstinumas ir operaciniai tikslai.

11.4. ES BDAR (2016/679)

11.4.1. 32 straipsnio 1 dalies b–d punktai: ši politika palaiko reikalavimą taikyti tinkamas technines ir organizacines priemones duomenų saugumui užtikrinti, ypač sistemų pakeitimų metu.

11.4.2. 25 straipsnis – Duomenų apsauga pagal projektavimą ir numatytuosius nustatymus: užtikrina, kad pakeitimai, darantys poveikį asmens duomenims, integruotų privatumo ir saugumo reikalavimus į projektavimą ir diegimą.

11.4.3. 78 konstatuojamoji dalis: reikalauja, kad duomenų valdytojai įgyvendintų mechanizmus, pavyzdžiui, pakeitimų kontrolės politikas, siekdami užtikrinti nuolatinį tvarkymo sistemų konfidencialumą, vientisumą ir atsparumą.

11.5. ES NIS2 direktyva (2022/2555)

11.5.1. 21 straipsnio 2 dalies a, b, d, e punktai: nustato techninių ir organizacinių priemonių reikalavimus IRT rizikai valdyti, įskaitant riziką, kylančią dėl sistemų pakeitimų, programinės įrangos atnaujinimų ir infrastruktūros modifikacijų.

11.6. ES DORA reglamentas (2022/2554)

11.6.1. 5 straipsnis – Valdysenos ir vidaus kontrolės sistema: ši politika įgyvendina operacinės rizikos valdymo principus, susijusius su IRT pakeitimais ir atnaujinimais.

11.6.2. 8 straipsnis – IRT rizikos valdymo sistema: nustato reikalavimą finansų subjektams valdyti visus IRT sistemoms poveikį darančius pakeitimus taikant struktūrizuotus pakeitimų valdymo procesus; tai šioje politikoje atspindima klasifikavimo, testavimo, grąžinimo atgal ir dokumentavimo reikalavimais.

11.6.3. 12 straipsnis – Pranešimas apie incidentus: užtikrina, kad nepavykę pakeitimai, sukėlę IRT sutrikimus, būtų atsekami, dokumentuoti ir, kai taikoma, apie juos būtų pranešama.

11.7. COBIT 2019

11.7.1. BAI06 – Valdomi IT pakeitimai: ši politika tiesiogiai įgyvendina BAI06 tikslus, nustatydama struktūrizuotas darbo eigas pakeitimų tvirtinimui, poveikio vertinimui, komunikacijai ir testavimui.

11.7.2. BAI02 – Valdomas reikalavimų apibrėžimas ir BAI03 – Valdomas sprendimų identifikavimas ir kūrimas: užtikrina, kad verslo inicijuojami pakeitimai būtų peržiūrimi ir įgyvendinami saugiai.

11.7.3. DSS01 – Valdomos operacijos: palaiko nuolatinį sistemų vientisumą vykdant pakeitimus.

11.7.4. MEA01 ir MEA03 – Stebėti, vertinti ir įvertinti veiksmingumą bei atitiktį: sudaro sąlygas nuolatinei pakeitimų valdymo politikos veiksmingumo ir jos laikymosi priežiūrai.