					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P05S					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 taikomais standartais ir reglamentais

Standartas / reglamentas	Skyrius / straipsnis	Pastaba
ISO/IEC 27001:2022	6.1, 8 skyriai	
ISO/IEC 27002:2022	8 kontrolės priemonės	
NIST SP 800-53 Rev. 5	CM-2–CM-5, CM-11	
ES NIS2 direktyva	21 straipsnio 2 dalies b punktas	
ES DORA reglamentas	6 straipsnio 9 dalis, 8 straipsnio 4 dalies b punktas	
COBIT 2019	BAI06, DSS	

1. Tikslas

1.1 Ši politika užtikrina, kad visi IT sistemų, konfigūracijų, verslo programų ar debesijos paslaugų pakeitimai prieš įgyvendinimą būtų suplanuoti, įvertinti rizikos požiūriu, ištestuoti ir patvirtinti.

1.2 Tikslas – sumažinti veiklos sutrikimus, saugumo riziką ir paslaugų nepasiekiamumą, nustatant supaprastintą, tačiau privalomą procesą, taikomą ir mažoms įmonėms, turinčioms ribotus išteklius.

1.3 Ši politika prisideda prie ISO/IEC 27001:2022 sertifikavimo, formalizuodama techninių ir veiklos pakeitimų valdymą bei jų dokumentavimą.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 darbuotojams ir padalinių vadovams, kurie inicijuoja arba įgyvendina pakeitimus;

2.1.2 išoriniams IT paslaugų teikėjams, valdantiems sistemas ar programinę įrangą;

2.1.3 bendrovės vadovui, atsakingam už bendrą pakeitimų tvirtinimą.

2.2 Politika apima šių sričių pakeitimus:

2.2.1 programinės įrangos (atnaujinimai, pataisos, naujos programos);

2.2.2 techninės įrangos (keitimas, atnaujinimas);

2.2.3 tinklo ir užkardų konfigūracijų;

2.2.4 debesijos paslaugų, naudotojų prieigos teisių ar tiekėjų integracijų;

2.2.5 kritinių verslo procesų, susijusių su informacinėmis sistemomis.

2.3 Į šios politikos taikymo sritį patenka tiek planuoti, tiek skubūs pakeitimai.

3. Tikslai

3.1 Užtikrinti, kad visi IT ir verslo sistemų pakeitimai būtų autorizuoti, dokumentuoti ir prireikus atkuriami į ankstesnę būseną.

3.2 Užkirsti kelią neplanuotoms prastovoms, duomenų praradimui ar saugumo incidentams, kuriuos sukelia nekontroliuojami pakeitimai.

3.3 Nustatyti paprastas ir nuosekliai taikomas pakeitimų pateikimo, tvirtinimo, testavimo ir atkūrimo į ankstesnę būseną procedūras.

3.4 Tvarkyti auditui tinkamą pakeitimų žurnalą, užtikrinantį veiklos atskaitomybę ir atitiktį reglamentavimo reikalavimams.

3.5 Sudaryti sąlygas rizika grindžiamam sprendimų priėmimui dėl reikšmingų ar jautrių pakeitimų.

4. Vaidmenys ir atsakomybės

4.1 Bendrovės vadovas

4.1.1 Prisiima galutinę atsakomybę už visus reikšmingus pakeitimus.

4.1.2 Peržiūri ir tvirtina neįprastus, kritinius arba didelės rizikos pakeitimus.

4.1.3 Kas ketvirtį arba po didelių incidentų peržiūri pakeitimų žurnalą.

4.2 IT pagalbos funkcija arba išorinis IT paslaugų teikėjas

4.2.1 Įgyvendina pakeitimus, įskaitant konfigūracijų atnaujinimą, pataisų diegimą ir sistemų migravimą.

4.2.2 Tvarko bazinį pakeitimų žurnalą, kuriame registruojamos datos, pakeitimų tipai, rezultatai ir tvirtintojai.

4.2.3 Prieš įgyvendinimą ištestuoja pakeitimus ir prireikus atlieka atkūrimo į ankstesnę būseną veiksmus.

4.2.4 Informuoja paveiktus naudotojus prieš reikšmingus pakeitimus ir po jų.

[... 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 Ši politika turi būti peržiūrima kasmet bendrovės vadovo arba paskirto IT kontaktinio asmens, siekiant užtikrinti jos suderinamumą su esamomis sistemomis, darbo procesais ir reglamentavimo reikalavimais.

9.2 Tarpinės peržiūros

9.2.1 Peržiūros taip pat turi būti inicijuojamos šiais atvejais:

9.2.1.1 saugumo incidentai, kilę dėl netinkamo pakeitimų valdymo;

9.2.1.2 naujų IT sistemų įdiegimas;

9.2.1.3 susijusių standartų, tokių kaip ISO, NIS2 ar DORA, pakeitimai.

9.3 Atnaujinimų dokumentavimas

9.3.1 Šios politikos pakeitimai turi būti valdomi taikant versijų kontrolę ir tvirtinami bendrovės vadovo. Kiekvienoje versijoje turi būti nurodyta data, pakeitimų santrauka ir tvirtintojas.

9.4 Politikos komunikavimas

9.4.1 Apie visus atnaujinimus turi būti pranešta visiems paveiktiems darbuotojams ir išoriniams paslaugų teikėjams. Dokumentacija turi būti atnaujinta visose susijusiose vietose (pvz., darbuotojų portale, bendrinamuose diskuose).

10. Susijusios politikos ir sąsajos

10.1 Ši politika glaudžiai susijusi su šiomis SME politikomis:

10.1.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: nustato pakeitimų tvirtinimo įgaliojimus.

10.1.2 P4S – Prieigos kontrolės politika: užtikrina, kad dėl pakeitimų atliekami prieigos pakeitimai būtų tinkamai dokumentuoti ir įgyvendinti.

10.1.3 P7S – Įdarbinimo ir darbo santykių nutraukimo politika: koordinuoja pakeitimus, susijusius su vaidmenų pasikeitimu ir prieigos suteikimu.

10.1.4 P15S – Atsarginių kopijų ir atkūrimo politika: užtikrina, kad nesėkmingo pakeitimo atveju būtų galima atlikti atkūrimą į ankstesnę būseną ir atkūrimą.

10.1.5 P30S – Reagavimo į incidentus politika: nustato, kaip nesėkmingi arba neautorizuoti pakeitimai tvarkomi kaip saugumo incidentai.

11. Nuorodiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 6.1 skyrius – rizika grindžiamas planavimas turi apimti su pakeitimais susijusią veiklą.

11.1.2 8.1 skyrius – veiklos kontrolės priemonės turi būti nuosekliai taikomos su pakeitimais susijusiai veiklai, siekiant užtikrinti paslaugų vientisumą.

11.2 ISO/IEC 27002

11.2.1 8.32 kontrolės priemonė – pateikia rekomendacijas dėl saugaus pakeitimų valdymo procesų, įskaitant dokumentavimą, testavimą ir tvirtinimą.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – bazinė sistemų konfigūracija prieš atliekant pakeitimą.

11.3.2 CM-3 – konfigūracijos pakeitimų kontrolė.

11.3.3 CM-4 – saugumo poveikio analizė.

11.3.4 CM-5 – pakeitimų tvirtinimas ir dokumentavimas.

11.3.5 CM-11 – pakeitimų auditas ir stebėsena.

11.4 ES NIS2 direktyva

11.4.1 21 straipsnio 2 dalies b punktas – reikalauja formalių techninių ir organizacinių saugumo priemonių procedūrų, įskaitant pakeitimų valdymą.

11.5 ES DORA reglamentas

11.5.1 6 straipsnio 9 dalis ir 8 straipsnio 4 dalies b punktas – reikalauja, kad finansų subjektai užtikrintų IRT sistemų pakeitimų ir konfigūracijų valdymą.

11.6 COBIT 2019

11.6.1 BAI06 – Pakeitimų valdymas: pabrėžia planavimą, rizikos vertinimą ir galimybę atkurti ankstesnę būseną.

11.6.2 DSS01 – Veiklos valdymas: užtikrina veiklos vientisumą techninių perėjimų ir pakeitimų metu.