					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P15S					Dokumento pavadinimas: **Atsarginių kopijų ir atkūrimo 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	Pastaba
ISO/IEC 27001:2022	8 skyrius	Atsarginių kopijų kontrolės priemonės pagal ISVS reikalavimus
ISO/IEC 27002:2022	Kontrolės priemonės 5.29, 8.13	Geriausioji atsarginių kopijų praktika, integracija su veiklos tęstinumu
NIST SP 800-53 Rev.5	CP-9, MP-6	Atsarginių kopijų ir laikmenų apsauga
ES NIS2 direktyva	21 straipsnio 2 dalies c punktas	Atsparumas ir veiklos tęstinumas taikant atsargines kopijas
ES DORA reglamentas	10 straipsnio 1 dalis	IRT tęstinumas – atsarginės kopijos finansų sektoriaus organizacijoms
COBIT 2019	BAI04.05, DSS04	Atsarginių kopijų dokumentavimas, testavimas ir procesų kontrolė
ES BDAR	5 straipsnio 1 dalies f punktas, 32 straipsnio 1 dalies c punktas	Duomenų vientisumas, prieinamumas ir savalaikis atkūrimas

1. Tikslas

1.1 Ši politika nustato, kaip organizacijoje vykdomas ir valdomas atsarginių kopijų darymas, siekiant užtikrinti veiklos tęstinumą, apsaugą nuo duomenų praradimo ir sudaryti sąlygas savalaikiam atkūrimui po incidentų.

1.2 Ji nustato privalomas taisykles, pagal kurias sistemos ir duomenys turi būti kopijuojami, saugomi ir atkuriami, ypač mažose ir vidutinėse įmonėse, neturinčiose sudėtingos IT infrastruktūros.

1.3 Ši politika padeda užtikrinti pasirengimą auditui ir ISO/IEC 27001 sertifikavimui, nustatydama, kad esminės atsarginių kopijų kontrolės priemonės būtų įdiegtos, taikomos nuosekliai ir reguliariai peržiūrimos.

1.4 Organizacijos gebėjimas atsigauti po techninių sutrikimų, atsitiktinio ištrynimo ar kibernetinių incidentų priklauso nuo griežto šios politikos laikymosi.

2. Taikymo sritis

2.1 Ši politika taikoma visoms verslo sistemoms ir duomenims, įskaitant:

2.1.1 finansinius įrašus, klientų informaciją ir žmogiškųjų išteklių duomenis;

2.1.2 stalinius kompiuterius, nešiojamuosius kompiuterius, serverius ir debesijos programas, naudojamas verslo operacijose;

2.1.3 atsarginių kopijų laikmenas, pavyzdžiui, USB laikmenas, išorines saugyklas ar debesijos aplinkoje saugomas atsargines kopijas.

2.2 Ji taip pat taikoma visiems asmenims, atsakingiems už atsarginių kopijų procesų vykdymą ar valdymą, įskaitant:

2.2.1 generalinį vadovą (GM) arba paskirtą atsakingą asmenį;

2.2.2 išorės IT paslaugų teikėjus ar konsultantus;

2.2.3 visus darbuotojus, atsakingus už duomenų saugojimą patvirtintose vietose.

3. Tikslai

3.1 Užtikrinti, kad visi kritiniai veiklos duomenys ir sistemos būtų saugiai kopijuojami tinkamu periodiškumu, atsižvelgiant į riziką ir veiklos poreikius.

3.2 Užtikrinti, kad po sutrikimų duomenys galėtų būti atkuriami savalaikiai ir visiškai.

3.3 Užkirsti kelią neteisėtai prieigai, manipuliavimui ar atsarginių kopijų duomenų praradimui taikant veiksmingas saugojimo kontrolės priemones.

3.4 Aiškiai priskirti vaidmenis ir atsakomybes už atsarginių kopijų procedūrų įgyvendinimą ir testavimą bei užtikrinti jų vykdymą.

3.5 Palaikyti atitiktį ISO/IEC 27001, ES BDAR ir kitiems taikytiniems reglamentavimo reikalavimams taikant struktūruotą ir dokumentuotą atsarginių kopijų praktiką.

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas (GM)

4.1.1 tvirtina šią politiką ir užtikrina jos įgyvendinimą;

4.1.2 skiria išteklius ir nustato atsakomybę už atsarginių kopijų ir atkūrimo veiklą;

4.1.3 peržiūri atsarginių kopijų nesėkmes, incidentus ir politikos neatitiktis;

4.1.4 atlieka kasmetines politikos peržiūras ir užtikrina pasirengimą auditui.

4.2 Išorės IT paslaugų teikėjas (jei taikoma)

4.2.1 įgyvendina ir valdo atsarginių kopijų sprendimus (vietinius arba debesijos aplinkoje);

4.2.2 stebi atsarginių kopijų vykdymo sėkmingumą ir planuoja atkūrimo testus;

4.2.3 apie nesėkmes ir incidentus tiesiogiai praneša GM;

4.2.4 užtikrina šifravimą, prieigos apribojimus ir tinkamą atsarginių kopijų laikmenų tvarkymą.

[... 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 GM turi peržiūrėti ne rečiau kaip kartą per metus. Tarpinių peržiūrų priežastys apima:

9.1.1 esminius sistemų ar saugojimo metodų pokyčius;

9.1.2 naujų debesijos ar IT platformų įdiegimą;

9.1.3 teisinius ar reglamentavimo pokyčius, darančius poveikį duomenų atkūrimui;

9.1.4 audito išvadas ar incidentus.

9.2 GM atsako už peržiūros inicijavimą, pakeitimų tvirtinimą ir atnaujinimų komunikavimą.

9.3 Politikos versijos turi būti sekamos ir archyvuojamos. Nebegaliojančių versijų prieiga turi būti ribojama, kad audito ar veiklos atkūrimo metu nekiltų painiava.

10. Susijusios politikos ir sąsajos

10.1 Ši politika yra suderinta su toliau nurodytomis SME politikomis ir nuo jų priklauso:

10.1.1 P14S – Duomenų saugojimo ir sunaikinimo politika: nustato, kiek laiko atsarginių kopijų duomenys turi būti saugomi ir kaip jie turi būti saugiai ištrinami.

10.1.2 P13S – Duomenų klasifikavimo ir ženklinimo politika: padeda nustatyti, kuriems duomenims turi būti teikiama pirmenybė darant atsargines kopijas pagal klasifikavimo lygius.

10.1.3 P30S – Reagavimo į incidentus politika: apima procedūras tais atvejais, kai atsarginės kopijos nesuveikia arba kai po pažeidimo ar nepasiekiamumo būtinas duomenų atkūrimas.

10.1.4 P2S – Valdysenos vaidmenų ir atsakomybių politika: priskiria aiškius įgaliojimus atsarginių kopijų priežiūrai ir politikos įgyvendinimui.

10.1.5 P17S – Duomenų apsaugos ir privatumo politika: užtikrina, kad su asmens duomenimis susijęs atsarginių kopijų tvarkymas atitiktų teisinius ir privatumo reikalavimus.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8.1 skyrius: atsarginių kopijų sistemų operacinis planavimas ir kontrolė kaip ISVS dalis.

11.2 ISO/IEC 27002

11.2.1 Kontrolė 8.13: nustato gerąją atsarginių kopijų planavimo, stebėsenos ir atkūrimo praktiką.

11.2.2 Kontrolė 5.29: atsarginių kopijų integravimas su veiklos tęstinumu ir pasirengimu atkūrimui.

11.3 NIST SP 800-53 Rev.5

11.3.1 CP-9 (Nenumatytų atvejų planavimas): nustato struktūruotas atsarginių kopijų strategijas veiklos atsparumui užtikrinti.

11.3.2 MP-6 (Laikmenų apsauga): reikalauja saugaus atsarginių kopijų laikmenų tvarkymo ir sunaikinimo.

11.4 ES BDAR

11.4.1 5 straipsnio 1 dalies f punktas: nustato asmens duomenų vientisumo ir prieinamumo reikalavimą.

11.4.2 32 straipsnio 1 dalies c punktas: reikalauja galimybės laiku atkurti prieigą prie asmens duomenų.

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies c punktas: reikalauja atsarginių kopijų ir atkūrimo kaip atsparumo ir veiklos tęstinumo planavimo dalies.

11.6 ES DORA reglamentas

11.6.1 10 straipsnio 1 dalis: finansų sektoriaus organizacijos turi užtikrinti atsargines kopijas kaip IRT tęstinumo priemonių dalį.

11.7 COBIT 2019

11.7.1 BAI04.05: reikalauja dokumentuotų atsarginių kopijų strategijų.

11.7.2 DSS04.07: pabrėžia reguliarų testavimą ir atsarginių kopijų bei duomenų atkūrimo procesų kontrolę.