					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P15					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	Punktas / straipsnis	Komentaras
ISO/IEC 27001:2022	6.1.3, 8 punktai	Rizikos tvarkymas, planavimas ir operacinės atsarginių kopijų kontrolės priemonės
ISO/IEC 27002:2022	Kontrolės priemonės 8.13, 5.28, 5.29	Atsarginių kopijų valdymas, saugus sunaikinimas ir atsparumas
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Sistemų atsarginių kopijų, atkūrimo ir laikmenų saugaus išvalymo reikalavimai
ES BDAR	32 straipsnis, 49 konstatuojamoji dalis	Asmens duomenų atkūrimas ir prieinamumas, veiklos tęstinumas
ES NIS2 direktyva	21 straipsnio 2 dalies c–e punktai	Atsarginių kopijų ir veiklos tęstinumo kontrolės priemonės atsparumui užtikrinti
ES DORA reglamentas	10, 11 straipsniai	Finansų sektoriaus atsarginių kopijų, atkūrimo ir testavimo reikalavimai
COBIT 2019	DSS01, DSS04, MEA03	Atsarginių kopijų operacijos, veiklos tęstinumas ir atitikties stebėsena

1. Tikslas

1.1 Šios politikos tikslas – nustatyti privalomuosius reikalavimus duomenų, sistemų ir taikomųjų programų atsarginių kopijų kūrimui ir atkūrimui, siekiant užtikrinti operacinį atsparumą, duomenų vientisumą ir veiklos tęstinumą.

1.2 Politika nustato standartizuotą sistemą, skirtą:

1.2.1 apsaugoti organizacijos duomenis nuo praradimo dėl ištrynimo, sugadinimo, gedimo ar kibernetinių atakų;

1.2.2 apibrėžti atkūrimo reikalavimus pagal aiškiai nustatytus RTO (atkūrimo laiko tikslas) ir RPO (atkūrimo taško tikslas) parametrus;

1.2.3 integruoti atsarginių kopijų operacijas į platesnę informacijos saugumo valdymo sistemą (ISVS) ir veiklos tęstinumo planus (BCP/DRP);

1.2.4 užtikrinti atitiktį taikomiems įstatymams ir sektoriaus reglamentavimo reikalavimams dėl prieinamumo ir atkuriamumo.

1.3 Ši politika įgyvendina ISO/IEC 27001:2022 kontrolės priemones, susijusias su saugiu duomenų sunaikinimu (5.28), atsparumu (5.29) ir informacijos atsarginėmis kopijomis (8.13), taip pat atitinka gerąją praktiką, nustatytą ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, ES BDAR, DORA reglamente ir NIS2 direktyvoje.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 visoms verslui kritinėms ir operacinėms sistemoms, patenkančioms į informacijos saugumo valdymo sistemos taikymo sritį;

2.1.2 visiems struktūrizuotiems duomenims ir nestruktūrizuotiems veiklos duomenims, įskaitant duomenų bazes, failus, el. laiškus ir konfigūracijas;

2.1.3 visoms aplinkoms – vietinei infrastruktūrai, debesijos aplinkoms, hibridinėms aplinkoms ir nuotoliniam / išoriniam saugojimui;

2.1.4 visam personalui, atsakingam už atsarginių kopijų procesų valdymą, vykdymą, tikrinimą ar atkūrimą.

2.2 Ji taip pat taikoma:

2.2.1 atsarginių kopijų laikmenoms ir infrastruktūrai, įskaitant fizines juostas, virtualius įrenginius, diskų momentines kopijas ir debesijos aplinkoje veikiančius atsarginių kopijų sprendimus;

2.2.2 trečiųjų šalių paslaugų teikėjams, su kuriais sudarytos sutartys dėl organizacijos atsarginių kopijų talpinimo, valdymo ar tvarkymo;

2.2.3 žurnalų, konfigūracijų, audito pėdsakų ir veiklos tęstinumui svarbios operacinės dokumentacijos atsarginėms kopijoms.

2.3 Sistemos, kurioms atsarginės kopijos aiškiai netaikomos, turi būti dokumentuotos, joms turi būti atliktas rizikos vertinimas, o tokia išimtis turi būti formaliai patvirtinta ISVS vadovo ir sistemos savininko.

3. Tikslai

3.1 Užtikrinti, kad visų kritinių sistemų ir duomenų atsarginės kopijos būtų kuriamos patikimai, pakankamu dažniu ir taikant tinkamą perteklinį kopijavimą bei saugumo kontrolės priemones.

3.2 Nustatyti atkūrimo mechanizmus, atitinkančius apibrėžtus RTO ir RPO reikalavimus pagal verslo poveikio vertinimus.

3.3 Užtikrinti išsamią atsarginių kopijų procedūrų, saugojimo terminų, vaidmenų ir technologijų dokumentaciją.

3.4 Patvirtinti atsarginių kopijų operacijų veiksmingumą sistemingai testuojant atkūrimą, registruojant nesėkmes žurnaluose ir stebint taisomuosius veiksmus.

3.5 Apsaugoti atsarginių kopijų duomenis nuo neteisėtos prieigos, keitimo ar sunaikinimo per visą jų gyvavimo ciklą.

3.6 Užtikrinti atitiktį:

3.6.1 ISO/IEC 27001 operacinėms ir veiklos tęstinumo kontrolės priemonėms;

3.6.2 NIST SP 800-53 CP ir MP šeimų reikalavimams dėl atsarginių kopijų ir saugaus išvalymo;

3.6.3 ES BDAR 32 straipsniui ir 49 konstatuojamajai daliai dėl asmens duomenų atkūrimo ir prieinamumo;

3.6.4 DORA reglamento 10 straipsniui ir NIS2 direktyvos 21 straipsniui dėl IRT veiklos tęstinumo ir atsparumo.

3.7 Užtikrinti, kad trečiųjų šalių atsarginių kopijų paslaugos atitiktų sutartinius ir reglamentavimo saugumo įpareigojimus, įskaitant šifravimo, sunaikinimo ir pranešimų teikimo reikalavimus.

4. Vaidmenys ir atsakomybės

4.1 Vadovybė

4.1.1 Tvirtina šią politiką ir užtikrina, kad verslui kritinės sistemos būtų tinkamai apsaugotos taikant patvirtintą atsarginių kopijų kūrimo ir atkūrimo praktiką.

4.1.2 Užtikrina, kad atsarginių kopijų operacijoms būtų skirta pakankamai išteklių ir kad jos būtų periodiškai peržiūrimos atitikties reglamentavimo reikalavimams užtikrinti.

4.2 Informacijos saugumo vadovas (CISO)

4.2.1 Valdo šią politiką ir užtikrina jos suderinamumą su platesne informacijos saugumo, rizikos ir veiklos tęstinumo valdymo sistema.

4.2.2 Prižiūri atsarginių kopijų procedūrų integravimą į BCP/DRP, reagavimo į incidentus procesus ir atsparumo planavimą.

4.2.3 Peržiūri atsarginių kopijų išimtis ir vertina rizikos priėmimo pasiūlymus dėl kritinių sistemų neįtraukimo.

[... 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 bent kartą per metus arba anksčiau, jei tai lemia:

9.1.1 veiklos tęstinumo arba atkūrimo po katastrofos strategijos pokyčiai;

9.1.2 nauji reglamentavimo ar teisiniai įpareigojimai, turintys įtakos atsarginių kopijų dažniui ar duomenų saugojimui;

9.1.3 sistemos architektūros, atsarginių kopijų įrankių ar paslaugų teikėjų pokyčiai;

9.1.4 reikšmingi incidentai arba audito išvados, susijusios su duomenų praradimu ar atkūrimo nesėkmėmis.

9.2 Peržiūrą koordinuoja CISO, bendradarbiaudamas su:

9.2.1 IT infrastruktūros ir operacijų komanda;

9.2.2 vidaus audito / atitikties funkcija;

9.2.3 duomenų apsaugos pareigūnu (DAP);

9.2.4 veiklos tęstinumo ir atkūrimo po katastrofos komandomis.

9.3 Atsarginių kopijų grafikai, sistemų įtraukimo sąrašai, atkūrimo dokumentacija ir išimčių žurnalai turi būti peržiūrimi lygiagrečiai, siekiant užtikrinti:

9.3.1 viso kritinio turto atsarginių kopijų aprėpties tikslumą;

9.3.2 atitiktį RTO/RPO ir saugojimo reikalavimams;

9.3.3 testavimo žurnalų ir incidentų ataskaitų išsamumą;

9.3.4 anksčiau nustatytų kontrolės priemonių spragų pašalinimą.

9.4 Visi atnaujinimai privalo:

9.4.1 būti valdomi pagal versijų kontrolę ir saugomi ISVS dokumentų saugykloje;

9.4.2 apimti pakeitimų santrauką ir pagrindimą;

9.4.3 būti patvirtinti vadovybės;

9.4.4 būti komunikuojami visam paveiktam techniniam ir verslo personalui.

10. Susijusios politikos ir sąsajos

10.1 Ši politika tiesiogiai palaiko ir yra susijusi su šiais dokumentais:

10.1.1 P6 - Rizikos valdymo politika: nustato rizika grindžiamą atsarginių kopijų apsaugos prioritetų taikymą sistemoms ir paslaugoms.

10.1.2 P12 - Turto valdymo politika: užtikrina, kad sistemoms, kurioms taikomos atsarginės kopijos, būtų tvarkoma turto apskaita ir jos būtų susietos su gyvavimo ciklo stebėsena bei klasifikavimu.

10.1.3 P13 - Duomenų klasifikavimo ir ženklinimo politika: nustato, kurioms duomenų kategorijoms reikalingos atsarginės kopijos, įskaitant ženklinimo metaduomenis prioritetams nustatyti.

10.1.4 P14 - Duomenų saugojimo ir sunaikinimo politika: suderina atsarginių kopijų saugojimą su reglamentavimo saugojimo ribomis ir tinkamu pasibaigusio galiojimo laikmenų sunaikinimu.

10.1.5 P16 - Duomenų maskavimo ir pseudonimizavimo politika: palaiko duomenų minimizavimą kuriant jautrių duomenų rinkinių atsargines kopijas.

10.1.6 P30 - Reagavimo į incidentus politika: taikoma atsarginių kopijų nesėkmių, atkūrimo problemų ar atsarginių kopijų duomenų saugyklų kompromitavimo atvejais.

10.2 Šios tarpusavyje susietos politikos sudaro vientisą sistemą, užtikrinančią, kad atsarginių kopijų valdysena būtų integruota į platesnę organizacijos ISVS ir operacinio atsparumo strategiją.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001:

11.1.1 6.1.3 punktas – Rizikos tvarkymo planas: palaiko rizika grindžiamą atsarginių kopijų prioritetų nustatymą ir atkūrimo planavimą.

11.1.2 8.1 punktas – Operacinis planavimas ir kontrolė: integruoja atkūrimo ir veiklos tęstinumo kontrolės priemones kaip operacinių apsaugos priemonių dalį.

11.1.3 A priedo 5.28 kontrolės priemonė – Saugus įrangos sunaikinimas arba pakartotinis naudojimas: apima saugų atsarginių kopijų laikmenų išvalymą.

11.1.4 A priedo 5.29 kontrolės priemonė – Informacijos saugumas sutrikimo metu: užtikrina atkūrimo galimybes incidentų ar katastrofų metu.

11.1.5 A priedo 8.13 kontrolės priemonė – Informacijos atsarginės kopijos: tiesiogiai įgyvendinama planinėmis, testuojamomis ir saugiomis atsarginių kopijų operacijomis.

11.2 ISO/IEC 27002:2022 – 8.13, 5.28, 5.29 kontrolės priemonės: šios kontrolės priemonės sustiprina reikalavimą reguliariai kurti atsargines kopijas, patvirtinti vientisumą ir planuoti atkūrimą visose IT aplinkose.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 – Sistemos atsarginė kopija: nustato išsamias atsarginių kopijų procedūras, įskaitant saugojimą išorinėje vietoje ir atkūrimo testavimą.

11.3.2 CP-10 – Sistemos atkūrimas ir atstatymas: reikalauja patvirtintų visiško arba dalinio atkūrimo procedūrų, suderintų su atkūrimo tikslais.

11.3.3 MP-6 – Laikmenų išvalymas: užtikrina saugų pasenusių atsarginių kopijų laikmenų tvarkymą.

11.3.4 SI-12 – Informacijos tvarkymo procedūros: sustiprina atsarginių kopijų kūrimo ir atkūrimo atsakomybes jautrių duomenų atžvilgiu.

11.4 ES BDAR (2016/679):

11.4.1 32 straipsnis – Tvarkymo saugumas: nustato atkūrimo galimybių ir duomenų prieinamumo apsaugos priemonių reikalavimą, ypač asmens duomenims.

11.4.2 49 konstatuojamoji dalis: palaiko veiklos tęstinumo ir atkūrimo po katastrofos priemones, įskaitant saugias atsargines kopijas kaip organizacijos atsparumo dalį.

11.5 ES NIS2 direktyva (2022/2555):

11.5.1 21 straipsnio 2 dalies c–e punktai: reikalauja techninių ir organizacinių priemonių, įskaitant atsarginių kopijų ir veiklos tęstinumo kontrolės priemones, siekiant užtikrinti paslaugų atsparumą.

11.6 ES DORA reglamentas (2022/2554):

11.6.1 10 straipsnis – IRT veiklos tęstinumas: reikalauja, kad finansų įstaigos užtikrintų išsamias duomenų atsargines kopijas, atkūrimą ir veiklos tęstinumo planavimą.

11.6.2 11 straipsnis – IRT veiklos tęstinumo planų testavimas: pabrėžia atkūrimo galimybių patvirtinimą reguliariu testavimu.

11.7 COBIT 2019:

11.7.1 DSS01 – Valdomos operacijos: palaiko patikimą paslaugų teikimą užtikrinant apsaugotą duomenų prieinamumą.

11.7.2 DSS04 – Valdomas veiklos tęstinumas: apibrėžia strategines ir operacines veiklos tęstinumo kontrolės priemones, įskaitant patvirtintas atsargines kopijas.

11.7.3 MEA03 – Atitikties stebėsena, vertinimas ir analizė: nustato periodinės veiklos tęstinumo priemonių peržiūros reikalavimą, įskaitant atsarginių kopijų kontrolės priemonių veiksmingumą.