					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: P32S					Dokumento pavadinimas: **Veiklos tęstinumo ir atkūrimo po katastrofos 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	6.1, 6.3, 8 skyriai	
ISO/IEC 27002:2022	Kontrolės priemonės 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
ES BDAR	32, 33 straipsniai	
ES NIS2 direktyva	21 straipsnio 2 dalies f punktas	
ES DORA reglamentas	10 straipsnis	
COBIT 2019	DSS	

1. Tikslas

1.1 Ši politika užtikrina, kad organizacija galėtų tęsti veiklą ir atkurti esmines IT paslaugas trikdžių metu ir po jų, įskaitant elektros energijos tiekimo sutrikimus, kibernetines atakas, išpirkos reikalaujančių programų infekcijas ar sistemų gedimus.

1.2 Joje nustatoma aiški veiklos tęstinumo ir atkūrimo po katastrofos (BC/DR) planavimo sistema, pritaikyta MVĮ, neturinčioms dedikuotų IT komandų.

1.3 Ši politika padeda organizacijai vykdyti taikomus ISO/IEC 27001:2022, ES BDAR, NIS2 direktyvos, DORA reglamento ir COBIT 2019 reikalavimus, kartu stiprinant operacinį atsparumą ir klientų pasitikėjimą.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 visoms verslui kritinėms sistemoms ir paslaugoms (pvz., el. paštui, debesijos saugykloms, sąskaitų išrašymo platformoms, klientų įrašams)

2.1.2 visiems darbuotojams ir išorės IT paslaugų teikėjams, atsakingiems už BC/DR pasirengimą ir vykdymą

2.1.3 visų rūšių trikdžiams, įskaitant kibernetinius incidentus, aparatinės įrangos gedimus, elektros energijos tiekimo sutrikimus, užliejimą ir negalėjimą patekti į biurą

2.2 Ši politika apima:

2.2.1 atsarginių kopijų valdymą

2.2.2 veiklos tęstinumo planavimą (BCP)

2.2.3 atkūrimo po katastrofos veiklą

2.2.4 darbuotojų mokymą ir testavimą

2.2.5 reagavimo į teisinius ir reguliacinius reikalavimus procedūras

3. Tikslai

3.1 Apsaugoti organizacijos gebėjimą teikti pagrindines paslaugas nepaisant neplanuotų trikdžių.

3.2 Užtikrinti savalaikį sistemų ir duomenų atkūrimą pagal iš anksto nustatytus atkūrimo laiko tikslus (RTO).

3.3 Sudaryti sąlygas visam personalui krizių metu laikytis veiklos tęstinumo procedūrų, mažinant neapibrėžtumą.

3.4 Užtikrinti atitiktį duomenų apsaugą ir operacinį atsparumą reglamentuojantiems teisės aktams, įskaitant ES BDAR 32 straipsnį ir NIS2 direktyvos 21 straipsnį.

3.5 Nustatyti praktinę ir testuojamą veiklos tęstinumo ir atkūrimo strategiją, tinkamą MVĮ.

4. Vaidmenys ir atsakomybės

4.1 Generalinis direktorius (GD)

4.1.1 Atsako už BC/DR procesą ir šią politiką.

4.1.2 Tvirtina veiklos tęstinumo planą (BCP).

4.1.3 Koordinuoja reagavimą į incidentus ir vidinę komunikaciją trikdžių metu.

4.1.4 Prireikus teikia pranešimus reguliavimo ir priežiūros institucijoms (pvz., apie ES BDAR pažeidimus).

4.2 Išorės IT paslaugų teikėjas / sistemų administratorius

4.2.1 Prižiūri ir testuoja atsargines kopijas.

4.2.2 Suveikus aktyvavimo sąlygoms vykdo atkūrimo po katastrofos procedūras.

4.2.3 Dokumentuoja visus atkūrimo veiksmus ir sistemų atkūrimo įvykius.

4.2.4 Nedelsdamas praneša GD apie kritinius IT incidentus.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Metinė politikos ir plano peržiūra

9.1.1 Generalinis direktorius (GD) privalo užtikrinti, kad ši politika ir su ja susijęs veiklos tęstinumo planas (BCP) būtų formaliai peržiūrimi bent kartą per metus.

9.1.2 Peržiūra turi apimti:

9.1.2.1 naujų arba didėjančių rizikų vertinimą

9.1.2.2 pakartotinį RTO/RPO patvirtinimą

9.1.2.3 tiekėjų ir kontaktinės informacijos patikrinimą

9.1.2.4 suderinimą su IT sistemų, teisinių įpareigojimų arba veiklos pokyčiais

9.2 Įvykiais grindžiami atnaujinimai

9.2.1 Ši politika taip pat turi būti atnaujinama reaguojant į:

9.2.1.1 esminius incidentus arba veiklos sutrikimus, ypač jei tikslai nebuvo pasiekti

9.2.1.2 naujus teisinius arba reguliacinius reikalavimus (pvz., DORA reglamento pakeitimus)

9.2.1.3 kritinių sistemų, debesijos platformų arba personalo pokyčius

9.2.1.4 kasmetinių BCP / DR testų išvadas

9.3 Pakeitimų kontrolės procesas

9.3.1 Visi pakeitimai turi būti tvirtinami GD.

9.3.2 Turi būti tvarkomas versijų istorijos žurnalas, įskaitant datą, pakeitimo aprašymą ir tvirtinantį asmenį.

9.3.3 Atnaujinta politika turi būti pakartotinai išplatinta visam susijusiam personalui, įskaitant IT paslaugų teikėją ir padalinių vadovus.

9.4 Įgytos patirties dokumentavimas

9.4.1 Po testų arba realių trikdžių dokumentuota įgyta patirtis turi būti panaudota būsimoms peržiūroms.

9.4.2 Šios peržiūros taip pat turi apimti tiekėjų veiksmingumo vertinimus ir reagavimo pakankamumo patikras.

10. Susijusios politikos ir sąsajos

10.1 Ši politika yra glaudžiai susieta su toliau nurodytomis MVĮ politikomis:

10.1.1 P1S – Informacijos saugumo politika: nustato aukšto lygmens saugumo tikslus, kuriuos turi palaikyti veiklos tęstinumo ir atkūrimo praktika.

10.1.2 P4S – Prieigos kontrolės politika: sudaro sąlygas avariniam naudotojų prieigos teisių atšaukimui arba atkūrimui veiklos sutrikimų scenarijuose.

10.1.3 P6S – Rizikos valdymo politika: sudaro pagrindą su veiklos tęstinumu susijusių rizikų identifikavimui, vertinimui ir prioritetų nustatymui.

10.1.4 P8S – Informacijos saugumo supratimo ugdymo ir mokymų politika: užtikrina, kad darbuotojai būtų pasirengę veikti trikdžių metu ir suprastų BCP.

10.1.5 P15S – Atsarginių kopijų ir atkūrimo politika: nustato konkrečias technines procedūras duomenų prieinamumui ir atkūrimui užtikrinti.

10.1.6 P17S – Duomenų apsaugos ir privatumo politika: užtikrina, kad veiklos tęstinumo planavimas užtikrintų asmens duomenų apsaugą ir atitiktų ES BDAR reikalavimus incidentų metu ir po jų.

10.1.7 P22S – Žurnalų tvarkymo ir stebėsenos politika: padeda aptikti įvykius, galinčius inicijuoti BC/DR procesus, ir po trikdžių pateikia kriminalistiniam auditui tinkamą audito pėdsaką.

10.1.8 P30S – Reagavimo į incidentus politika: kibernetinių ar operacinių incidentų atveju tiesiogiai taikoma prieš aktyvuojant atkūrimo procesą.

10.1.9 P31S – Įrodymų rinkimo ir kriminalistikos politika: užtikrina, kad veiklos tęstinumo scenarijų metu būtų surinkti skaitmeniniai kriminalistiniai įrodymai atitikties, draudimo arba tyrimo tikslais.

10.2 Šios politikos sudaro nuoseklią, auditui parengtą sistemą, skirtą atsparumui, atskaitomybei ir kontrolės priemonių tęstinumui visoje MVĮ veikloje užtikrinti.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001:

11.1.1 6.1 skyriuje reikalaujama rizika grindžiamo planavimo ir rizikos tvarkymo, įskaitant veiklos tęstinumą ir atkūrimą.

11.1.2 6.3 skyriuje pabrėžiamas nuolatinis tobulinimas po trikdžių.

11.1.3 8.1 skyriuje nustatomos operacinės kontrolės priemonės, apimančios ir dokumentuotas veiklos tęstinumo priemones.

11.2 ISO/IEC 27002:

11.2.1 Kontrolės priemonė 5.29 reikalauja nustatyti ir prižiūrėti veiklos tęstinumo priemones.

11.2.2 Kontrolės priemonė 5.30 reikalauja šių priemonių testavimo ir peržiūros.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 apibrėžia nenumatytų atvejų planavimo reikalavimus.

11.3.2 CP-4 nustato organizacijos personalo mokymo dėl nenumatytų atvejų reikalavimą.

11.3.3 CP-6 apima alternatyvios saugojimo vietos reikalavimus.

11.3.4 CP-7 nustato alternatyvios tvarkymo vietos reikalavimus.

11.4 ES BDAR:

11.4.1 32 straipsnyje reikalaujama priemonių, užtikrinančių nuolatinį tvarkymo sistemų ir paslaugų prieinamumą bei atsparumą.

11.4.2 33 straipsnis nustato pranešimo apie pažeidimą pareigas tais atvejais, kai veiklos tęstinumo sutrikimas lemia asmens duomenų pažeidimą.

11.5 ES NIS2 direktyva (2022/2555):

11.5.1 21 straipsnio 2 dalies f punktas reikalauja veiklos tęstinumo planavimo ir krizių valdymo pajėgumų kaip kibernetinės rizikos pasirengimo sąlygos.

11.6 ES DORA reglamentas (2022/2554):

11.6.1 10 straipsnyje reikalaujama įgyvendinti skaitmeninio operacinio atsparumo testavimo ir atkūrimo pajėgumus, ypač finansų sektoriaus MVĮ.

11.7 COBIT 2019:

11.7.1 DSS04 – Tęstinumo valdymas: pateikia įmonės valdysenos gaires operaciniam atsparumui palaikyti ir validuoti, įskaitant atsakomybių priskyrimą, testavimą, tiekėjų integraciją ir peržiūras po įvykio.