| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Čia įrašykite registruoto juridinio asmens pavadinimą | | | | | | |
| Dokumento numeris:<br>P32 | | | | | Dokumento pavadinimas:<br>**Veiklos tęstinumo ir atkūrimo po nelaimės politika** | | | | | | |
| Versija:<br>1.0 | | Įsigaliojimo data:<br>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** |
| | | | |
| | | | |

**Teisinis pranešimas (autorių teisės ir naudojimo apribojimai)**
(C) 2025 Clarysec LLC. All rights reserved.

Šis dokumentas yra Clarysec LLC intelektinė nuosavybė. Jokia šio dokumento dalis negali būti kopijuojama, pakartotinai naudojama, platinama ar keičiama komerciniais ar įgyvendinimo tikslais be išankstinio aiškaus rašytinio leidimo.
Neautorizuotas naudojimas yra griežtai draudžiamas ir gali užtraukti teisinius veiksmus.
Dėl licencijavimo kreipkitės: info@clarysec.com

Suderinta su standartais ir reglamentais

| Standartas / reglamentas | Punktas / straipsnis | Pastaba |
|---|---|---|
| ISO/IEC 27001:2022 | 8 skyrius | |
| ISO/IEC 27002:2022 | Kontrolės priemonės 5.29, 5.30 | |
| NIST SP 800-53 Rev.5 | CP-1–CP-11 | |
| NIST SP 800-34 Rev.1 | Nenumatytų atvejų planavimas | Gairės |
| ISO 22301:2019 | | Veiklos tęstinumo valdymo sistemos reikalavimai |
| ES BDAR | 32 straipsnis | |
| ES NIS2 direktyva | 21 straipsnio 2 dalies f punktas | |
| ES DORA reglamentas | 10 straipsnis | |
| COBIT 2019 | DSS04 | |

**1. Tikslas**

1.1. Ši politika nustato privalomas kontrolės priemones ir atsakomybes, skirtas užtikrinti organizacijos gebėjimą palaikyti arba atkurti kritines verslo operacijas ir jas palaikančias IRT paslaugas įvykus veiklą trikdančiam incidentui ir po jo.

1.2. Ja siekiama apsaugoti gyvybę, veiklos stabilumą, teisinių prievolių vykdymą, įsipareigojimus klientams ir organizacijos reputaciją, užtikrinant atsparumą per proaktyvų planavimą ir patvirtintas atkūrimo galimybes.

1.3. Ši politika sudaro pagrindą organizacijos veiklos tęstinumo valdymo (BCM) ir atkūrimo po nelaimės (DR) sistemai, užtikrinant atitiktį taikomiems reguliavimo, sutartiniams ir pramonės reikalavimams.

**2. Taikymo sritis**

2.1. Ši politika taikoma visiems organizacijos padaliniams, informacinėms sistemoms, verslo procesams, darbuotojams ir trečiųjų šalių paslaugoms, kurios pagal verslo poveikio analizės (BIA) rezultatus yra priskirtos kritinėms arba esminėms.

**2.2. Politika apima:**

2.2.1. gamtinius ir žmogaus sukeltus trikdžius, įskaitant kibernetines atakas, infrastruktūros gedimus, duomenų centrų nepasiekiamumą, pandemijas ir tiekėjų paslaugų sutrikimus

2.2.2. veiklos tęstinumo planų (BCP/DRP) planavimą, testavimą ir nuolatinį tobulinimą

2.2.3. vaidmenis ir atsakomybes, susijusius su reagavimu į ekstremaliąsias situacijas, atkūrimo koordinavimu ir incidentų eskalavimu

2.3. Šios politikos nuostatos taikomos visiems darbuotojams, turintiems veiklos tęstinumo arba atkūrimo atsakomybių, įskaitant IT, verslo savininkus, krizių valdytojus ir tiekėjus.

**3. Tikslai**

3.1. Užtikrinti verslo operacijų ir paslaugų tęstinumą taikant iš anksto apibrėžtas ir ištestuotas procedūras, kuo labiau sumažinant veiklos, reputacinį ir teisinį poveikį.

3.2. Atkurti IRT paslaugas per nustatytus atkūrimo laiko tikslus ir atkūrimo taško tikslus, suderintus su verslo rizikos tolerancijos lygiais.

3.3. Priskirti atsakomybę už veiklos tęstinumo ir atkūrimo po nelaimės planavimą, vykdymą ir valdyseną visos organizacijos mastu.

3.4. Užtikrinti, kad veiklos tęstinumo gebėjimai būtų reguliariai testuojami, prižiūrimi ir tobulinami remiantis realistiniais scenarijais ir audito išvadomis.

3.5. Įvykdyti atitikties įpareigojimus pagal ISO, NIST, ES BDAR, DORA reglamentą ir NIS2 direktyvą, pagrindžiant deramą rūpestingumą veiklos atsparumo ir prieinamumo srityse.

**4. Vaidmenys ir atsakomybės**

**4.1. Vadovybė**

4.1.1. Tvirtina Veiklos tęstinumo ir atkūrimo po nelaimės politiką ir užtikrina jos strateginį suderinamumą.

4.1.2. Skiria biudžetą ir išteklius veiklos tęstinumui, reagavimui į ekstremaliąsias situacijas ir atkūrimo pratyboms užtikrinti.

**4.2. Veiklos tęstinumo vadovas**

4.2.1. Atsako už visos organizacijos BCP rengimą, priežiūrą ir veiklos tęstinumo testavimo koordinavimą.

4.2.2. Valdo BIA grafiką, organizuoja mokymus ir užtikrina, kad dokumentacija atitiktų atitikties reikalavimus.

[ ... 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 kasmet turi peržiūrėti veiklos tęstinumo vadovas ir informacijos saugumo vadovas (CISO), siekdami užtikrinti suderinamumą su:**

9.1.1. verslo operacijų, kritinių sistemų arba infrastruktūros pokyčiais

9.1.2. įgyta patirtimi po incidentų, auditų, stalo pratybų arba DR testų

9.1.3. atnaujintais reguliavimo arba sutartiniais įpareigojimais (pvz., DORA reglamentu, ES BDAR, klientų RTO / RPO reikalavimais)

9.1.4. organizacijos rizikos apetito arba veiklos tęstinumo strategijos pakeitimais

**9.2. Peržiūros turi apimti:**

9.2.1. planų aktualumo ir kontaktinių duomenų patvirtinimą

9.2.2. pakartotinį atkūrimo laiko tikslų, atkūrimo taško tikslų ir atkūrimo lygmenų nustatymo vertinimą

9.2.3. atsarginių kopijų ir DR paslaugų pajėgumo vertinimą

9.2.4. suinteresuotųjų šalių, vykdžiusių naujausius atkūrimo planus ar testus, grįžtamąjį ryšį

**9.3. Visi politikos pakeitimai turi būti:**

9.3.1. valdomi taikant versijų kontrolę, su dokumentuotu pagrindimu ir suinteresuotųjų šalių patvirtinimu

9.3.2. komunikuojami pagrindiniams darbuotojams ir komandoms kartu su atnaujintomis atsakomybėmis

9.3.3. atspindėti atnaujintuose mokymuose, informuotumo medžiagoje ir veiklos procedūrose

9.4. Neatidėliotini tarpiniai atnaujinimai turi būti skelbiami, jei įvyksta esminis organizacinis pokytis, atsiranda teisinis reikalavimas arba nustatoma kritinė išvada, dėl kurios esami planai ar politika tampa nebetinkami.

**10. Susijusios politikos ir sąsajos**

**10.1. Ši politika taikoma kartu su šiais pagrindiniais dokumentais:**

10.1.1. P1 – Informacijos saugumo politika: nustato reikalavimą užtikrinti rizika grindžiamą ir atsparią veiklą bet kokiomis sąlygomis.

10.1.2. P5 – Pakeitimų valdymo politika: užtikrina, kad visi su atkūrimu susiję konfigūracijų arba infrastruktūros pakeitimai būtų vykdomi pagal dokumentuotą ir patvirtintą darbo eigą.

10.1.3. P14 – Duomenų saugojimo ir sunaikinimo politika: reglamentuoja atsarginių laikmenų ir tęstinumo operacijose naudojamų atkurtų duomenų gyvavimo ciklą.

10.1.4. P15 – Atsarginių kopijų ir atkūrimo politika: nustato atsarginių kopijų dažnumo, saugumo ir atkūrimo patvirtinimo kontrolės priemones.

10.1.5. P18 – Kriptografinių kontrolės priemonių politika: užtikrina, kad atkūrimo procesuose būtų laikomasi šifravimo ir konfidencialumo standartų.

10.1.6. P22 – Žurnalų tvarkymo ir stebėsenos politika: padeda aptikti ir eskaluoti įvykius, darančius poveikį veiklos tęstinumui.

10.1.7. P30 – Reagavimo į incidentus politika: apibrėžia lokalizavimo, eskalavimo ir pagrindinės priežasties analizės procesus, suderintus su veiklos tęstinumo aktyvavimo kriterijais.

10.1.8. P33 – Audito ir atitikties stebėsenos politika: patvirtina veiklos tęstinumo ir atkūrimo praktikų vientisumą ir veiksmingumą sistemose bei procesuose.

## 11. Pamatiniai standartai ir sistemos

11.1. Ši politika suderinta su tarptautiniu mastu pripažintais veiklos tęstinumo ir atkūrimo po nelaimės standartais, palaikančiais audituojamumą, atsparumą ir teisinę atitiktį.

### 11.2. ISO/IEC 27002

11.2.1. A priedo kontrolės priemonė 5.29 – Informacijos saugumas trikdžių metu: reikalauja užtikrinti saugumo kontrolės priemonių tęstinumą nepalankiomis sąlygomis.

11.2.2. A priedo kontrolės priemonė 5.30 – IRT parengtis veiklos tęstinumui: nustato prievolę parengti, testuoti ir patvirtinti IRT atkūrimo galimybes.

### 11.3. ISO 22301:2019 – Veiklos tęstinumo valdymo sistemos

11.3.1. Nustato sistemą BCM praktikai sukurti, įgyvendinti ir palaikyti, suderintai su organizacijos tikslais ir rizikos slenksčiais.

### 11.4. NIST SP 800-34 Rev.1 – Nenumatytų atvejų planavimo gairės

11.4.1. Nustato gerąją praktiką IT sistemų nenumatytų atvejų planams, įskaitant veiklos tęstinumo strategijos rengimą, poveikio analizę ir planų testavimą.

### 11.5. ES BDAR (2016/679)

11.5.1. 32 straipsnis – Tvarkymo saugumas: reikalauja užtikrinti tvarkymo sistemų atsparumą ir savalaikį prieinamumo bei prieigos prie asmens duomenų atkūrimą po incidento.

### 11.6. ES NIS2 direktyva (2022/2555)

11.6.1. 21 straipsnio 2 dalies f punktas: nustato veiklos tęstinumo ir krizių valdymo priemones, skirtas tinklų ir informacinių sistemų saugumui palaikyti.

### 11.7. ES DORA reglamentas (2022/2554)

11.7.1. 10 straipsnis – IRT veiklos tęstinumas: reikalauja, kad finansų sektoriaus subjektai rengtų ir testuotų IRT tęstinumo planus, įskaitant rizika grindžiamus RTO / RPO ir perjungimo į atsarginę aplinką galimybes.

### 11.8. COBIT 2019

11.8.1. DSS04 – Tęstinumo valdymas: apima visus veiklos tęstinumo planavimo aspektus, įskaitant grėsmių nustatymą, poveikio analizę, atkūrimo strategiją ir reguliarų testavimą.