					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: P31					Dokumento pavadinimas: **Įrodymų rinkimo ir skaitmeninės kriminalistikos 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**

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	Skyrius / straipsnis	Komentaras
ISO/IEC 27001:2022	8 skyrius	
ISO/IEC 27002:2022	Kontrolės priemonės 5.25–5.27, 8	
ISO/IEC 27035:2016	1 ir 3 dalys	
NIST SP 800-53 Rev. 5	IR-1–IR-9, AU-6, PL-2	
NIST SP 800-101 Rev. 1	Mobiliųjų įrenginių ir laikmenų kriminalistika	Mobiliųjų įrenginių ir laikmenų kriminalistika
NIST SP 800-86	Kriminalistinių metodų integravimas	Kriminalistinių metodų integravimas į reagavimą į incidentus
ES BDAR	5, 33–34 straipsniai	
ES NIS2 direktyva	23 straipsnio 1–4 dalys	
ES DORA reglamentas	17 straipsnio 1–3 dalys	
COBIT 2019	DSS01.07, DSS05	

1. Tikslas

1.1 Ši politika nustato struktūrizuotą, teisiškai pagrįstą skaitmeninių įrodymų identifikavimo, surinkimo, išsaugojimo, analizės ir sunaikinimo sistemą faktinių ar įtariamų saugumo incidentų atvejais.

1.2 Ji užtikrina, kad kriminalistinio pasirengimo ir įrodymų tvarkymo procesai:

1.2.1 išsaugotų įrodymų vientisumą ir perdavimo grandinę

1.2.2 palaikytų vidaus tyrimus, teisminius procesus ir pranešimų teikimą reguliavimo institucijoms

1.2.3 atitiktų tarptautiniu mastu pripažintus kriminalistikos standartus ir teisinio priimtinumo kriterijus

1.3 Ši politika padeda įgyvendinti organizacijos įsipareigojimą užtikrinti aktyvų reagavimą į incidentus, teisinę atitiktį ir valdysenos skaidrumą, kartu kuo mažiau trikdant veiklą.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 visiems darbuotojams, rangovams, tiekėjams ir paslaugų teikėjams, vykdantiems sistemų administravimo, incidentų valdymo ar tyrimo veiklą

2.1.2 visiems galiniams įrenginiams, serveriams, taikomosioms programoms, tinklams ir debesijos platformoms, kurias organizacija valdo arba už kurias atsako pagal sutartis

2.1.3 visiems incidentams ar įvykiams, kai būtinas įrodymų tvarkymas, įskaitant:

2.1.3.1 vidines grėsmes, duomenų saugumo pažeidimus ar sukčiavimo tyrimus

2.1.3.2 netinkamą sistemų ar prisijungimo duomenų naudojimą

2.1.3.3 operacinių technologijų (OT) ar pramoninio valdymo incidentus

2.1.3.4 fizinės prieigos pažeidimus, susijusius su skaitmeniniu turtu

2.2 Ši politika taip pat reglamentuoja bet kokią sąveiką su trečiųjų šalių kriminalistikos paslaugų teikėjais ar teisėsaugos institucijomis, kai byla perduodama teisiniam nagrinėjimui arba vykdomi reguliavimo procesai.

3. Tikslai

3.1 Sudaryti sąlygas greitam, saugiam ir su politika suderintam įrodymų surinkimui saugumo įvykių ar tyrimų metu.

3.2 Išsaugoti surinktų skaitmeninių įrodymų vientisumą, autentiškumą ir priimtinumą, taikant griežtą prieigos kontrolę, žurnalų pildymą ir tikrinimo procedūras.

3.3 Užtikrinti, kad visa kriminalistinė veikla būtų koordinuojama pagal teisinius ir reguliavimo reikalavimus, įskaitant duomenų apsaugą, darbo teisę ir tarptautinių duomenų perdavimų apribojimus.

3.4 Palaikyti po incidento atliekamą analizę, pirminės priežasties nustatymą ir kontrolės priemonių tobulinimą, remiantis aukštos kokybės kriminalistiniais rezultatais.

3.5 Integruoti kriminalistinį pasirengimą į bendrą informacijos saugumo valdymo sistemą (ISVS), palaikant auditus, pranešimus apie pažeidimus ir vadovybės sprendimų priėmimą.

4. Vaidmenys ir atsakomybės

4.1 Vyriausiasis informacijos saugumo pareigūnas

4.1.1 valdo šią politiką ir užtikrina, kad visos kriminalistinės operacijos būtų teisiškai pagrįstos, audituojamos ir grindžiamos rizika

4.1.2 tvirtina eskalavimą išorės teisiniams subjektams ir kriminalistikos paslaugų teikėjams

4.2 Kriminalistikos analitikai / incidentų valdytojai

4.2.1 vadovauja įrodymų surinkimui, išsaugojimui ir techninei analizei

4.2.2 užtikrina, kad perdavimo grandinė būtų tinkamai fiksuojama ir išlaikoma

4.2.3 dokumentuoja visus tyrimo metu atliktus veiksmus, išvadas ir naudotų priemonių nustatymus

[... 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 ne rečiau kaip kartą per metus ir prireikus atnaujinama, kad atspindėtų:

9.1.1 teisės aktų, reguliavimo reikalavimų ar teismų praktikos pokyčius, darančius poveikį kriminalistinėms procedūroms ar duomenų tvarkymui

9.1.2 pramonėje pripažintų kriminalistikos standartų ar priemonių atnaujinimus

9.1.3 įgytą patirtį iš poincidentinių peržiūrų, teisinių ginčų ar audito išvadų

9.1.4 technologinius pokyčius tiriamose platformose, įrenginiuose ar sistemose

9.2 Už peržiūros procesą atsako CISO, o procese turi būti konsultuojamasi su:

9.2.1 Teisės ir atitikties funkcijomis

9.2.2 duomenų apsaugos pareigūnu (DAP)

9.2.3 saugumo operacijų ir kriminalistikos komandomis

9.2.4 vidaus auditu

9.3 Visos peržiūrėtos redakcijos turi būti:

9.3.1 valdomos pagal versijų kontrolę ir saugomos politikų saugykloje

9.3.2 komunikuojamos paveiktoms suinteresuotosioms šalims, įskaitant kriminalistikos ir reagavimo komandas

9.3.3 papildytos susijusių veiklos procedūrų ir mokymo medžiagos atnaujinimais

9.4 Tarpinės peržiūros turi būti inicijuojamos po bet kokio kritinio incidento, susijusio su netinkamu įrodymų tvarkymu, perdavimo grandinės pažeidimu ar teisinio priimtinumo problemomis.

10. Susijusios politikos ir sąsajos

10.1 Ši politika yra suderinta su toliau nurodytomis organizacijos politikomis ir jomis grindžiama:

10.1.1 P1 – Informacijos saugumo politika: nustato bazinį įgaliojimą vykdyti tyrimus, valdyti įrodymus ir laikytis taikytinų teisės aktų.

10.1.2 P5 – Pakeitimų valdymo politika: užtikrina, kad aktyvių kriminalistinių procesų metu tiriamos sistemos nebūtų keičiamos.

10.1.3 P14 – Duomenų saugojimo ir sunaikinimo politika: reglamentuoja saugų įrodymų ir su bylomis susijusių duomenų sunaikinimą bei saugojimo terminus.

10.1.4 P18 – Kriptografinių kontrolės priemonių politika: nustato jautrių arba įrodomųjų duomenų saugojimo ir perdavimo šifravimo reikalavimus.

10.1.5 P22 – Žurnalų tvarkymo ir stebėsenos politika: užtikrina įvykių žurnalų ir telemetrijos prieinamumą įrodymų rinkimui ir kriminalistinei koreliacijai.

10.1.6 P30 – Reagavimo į incidentus politika: apibrėžia pirminio incidentų įvertinimo ir eskalavimo kelius, kuriais inicijuojamos kriminalistinės procedūros.

10.1.7 P33 – Audito ir atitikties stebėsenos politika: reguliariais auditais patvirtina kriminalistinių protokolų ir perdavimo grandinės reikalavimų laikymąsi.

11. Pamatiniai standartai ir sistemos

11.1 Ši politika yra suderinta su tarptautiniais kriminalistikos ir incidentų valdymo standartais, užtikrinant įrodymų vientisumą, teisinį pagrįstumą ir atitiktį skirtingose jurisdikcijose.

11.2 ISO/IEC 27001

11.2.1 8.1 skyrius – palaiko kriminalistinio pasirengimo ir įrodymų procedūrų operacinę kontrolę

11.3 ISO/IEC 27002

11.3.1 A priedo kontrolės priemonė 5.25 – atsakomybė už incidentų valdymą: reikalauja apibrėžtų vaidmenų tvarkant informacijos saugumo incidentus ir atliekant tyrimus.

11.3.2 A priedo kontrolės priemonė 5.26 – pranešimas apie informacijos saugumo įvykius: palaiko su įvykiais susijusių artefaktų rinkimą kaip įrodymus.

11.3.3 A priedo kontrolės priemonė 5.27 – reagavimas į informacijos saugumo incidentus: užtikrina struktūrizuotą, įrodymais grindžiamą šalinimą ir tyrimą.

11.3.4 A priedo kontrolės priemonė 8.27 – saugus kūrimas ir kriminalistika (kai taikoma): apima sistemų ir priemonių apsaugą tyrimų metu.

11.4 ISO/IEC 27035:2016 (1 ir 3 dalys)

11.4.1 Apibrėžia incidentų aptikimo, reagavimo ir kriminalistinio pasirengimo principus, įskaitant planavimą, perdavimo grandinę ir su incidentais susijusių įrodymų valdymą.

11.5 NIST SP 800-53 Rev. 5

11.5.1 IR-1–IR-9, AU-6, PL-2: apibrėžia struktūrizuotus reikalavimus planuoti, aptikti, analizuoti, lokalizuoti ir valdyti saugumo incidentus. Palaiko įrodymų rinkimą ir audituojamumą (AU-6) bei užtikrina suderinamumą su sistemų saugumo ir privatumo planais (PL-2) kriminalistinių tyrimų metu.

11.6 NIST SP 800-86

11.6.1 Pateikia gaires, kaip kriminalistinius procesus integruoti į platesnį reagavimo į incidentus gyvavimo ciklą ir užtikrinti kriminalistinį pasirengimą.

11.7 NIST SP 800-101 Rev. 1

11.7.1 Daugiausia dėmesio skiria gerajai praktikai, kaip teisiškai pagrįstu būdu surinkti, išsaugoti ir analizuoti skaitmeninių laikmenų bei mobiliųjų įrenginių įrodymus.

11.8 ES BDAR (2016/679)

11.8.1 5 straipsnis – su asmens duomenų tvarkymu susiję principai: taikomas įrodymams, kuriuose yra asmens ar jautrių duomenų, užtikrinant duomenų kiekio mažinimą ir tikslo apribojimą.

11.8.2 33–34 straipsniai – pranešimas apie asmens duomenų saugumo pažeidimą: kriminalistiniai duomenys padeda vykdyti pareigas pranešti apie pažeidimą ir užtikrinti teisinio atskleidimo procesus.

11.9 ES NIS2 direktyva (2022/2555)

11.9.1 23 straipsnis – pranešimo pareigos: kriminalistinė dokumentacija ir išvados padeda laiku ir tiksliai teikti incidentų ataskaitas kompetentingoms institucijoms.

11.10 ES DORA reglamentas (2022/2554)

11.10.1 17 straipsnis – pranešimas apie IRT incidentus: reikalauja išsamių pirminės priežasties ir įrodomųjų įrašų apie didelius su IRT susijusius incidentus, ypač finansų sektoriuje.

11.11 COBIT 2019

11.11.1 DSS01.07 – saugumo incidentų valdymas: nustato incidentų dokumentavimo ir tyrimo kruopštumo reikalavimus.

11.11.2 DSS05.04 – saugumo tyrimų valdymas: pabrėžia skaitmeninių įrodymų išsaugojimą ir paramą drausminiams bei teisiniams veiksmams.