					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: P31S					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**

Suderinta su standartais ir teisės aktais

Standartas / reglamentas	Punktas / straipsnis	Komentaras
ISO/IEC 27001:2022	6.1, 6.3, 8 skyriai	Rizika grindžiamas planavimas, gerinimo veiksmai ir operacinės kontrolės priemonės, skirtos įrodymų vientisumui užtikrinti
ISO/IEC 27002:2022	Kontrolės priemonės 5.24–5.27	Nustato saugų tvarkymą, peržiūras po incidentų ir įrodymais grindžiamą tobulinimą
ISO/IEC 27035-3:2016	6.3, 6.4, 7 skyriai	Užtikrina tinkamą planavimą, teisėtą rinkimą ir saugų skaitmeninių įrodymų tvarkymą, įskaitant perdavimo grandinės dokumentavimą
NIST SP 800-53 Rev. 5	IR-07, IR-08, AU-09, AU-12, PE-18	Pasirengimas skaitmeninei ekspertizei, audito žurnalų apsauga ir veiksminga integracija į reagavimą į incidentus
ES BDAR	33, 34 straipsniai	Asmens duomenų saugumo pažeidimų dokumentavimas ir atsekamumas
NIS2 direktyva	23 straipsnis	Atsekamas incidentų pranešimas ir saugus įrodymų tvarkymas
DORA reglamentas	17 straipsnio 1 ir 2 dalys	Užtikrina su IRT susijusių incidentų įrodymų rinkimą, saugojimą ir išlaikymą, skaitmeninės ekspertizės patikimumą ir galimybę atsakyti į reguliavimo užklausas
COBIT 2019	DSS05.06, DSS05.07	Patikimas žurnalų tvarkymas ir struktūruotas įrodymų valdymas saugiems, audituojamiems tyrimams

1. Tikslas

1.1. Ši politika nustato, kaip organizacija tvarko skaitmeninius įrodymus, susijusius su saugumo incidentais, asmens duomenų saugumo pažeidimais ar vidaus tyrimais. Ji užtikrina, kad įrodymai būtų renkami, saugomi ir išlaikomi teisiškai pagrįstu ir auditui tinkamu būdu, taip sudarant pagrindą tiek vidaus sprendimų priėmimui, tiek galimiems išoriniams veiksmams.

1.2. Ši politika leidžia mažoms organizacijoms apsaugoti žurnalų, rinkmenų ir sistemų atvaizdų vientisumą, kartu įrodant tinkamą rūpestingumą pagal ISO/IEC 27001, ES BDAR ir susijusius standartus.

1.3. Ji padeda užtikrinti pasirengimą skaitmeninei ekspertizei, nereikalaujant pažangių techninių išteklių ar visą darbo dieną dirbančios IT komandos, nes apibrėžia aiškias atsakomybes, procesus ir saugojimo terminus.

2. Taikymo sritis

2.1. Ši politika taikoma:

2.1.1. Visiems darbuotojams, IT paslaugų teikėjams ir išorės konsultantams, dalyvaujantiems reagavimo į incidentus, tyrimo ar pažeidimų analizės veiklose

2.1.2. Visoms bendrovės sistemoms, įskaitant nešiojamuosius kompiuterius, mobiliuosius įrenginius, serverius, el. pašto paskyras, SaaS platformas ir debesijos saugyklas (pvz., „Microsoft 365“, „Google Workspace“)

2.1.3. Bet kuriam įvykiui, kuriam reikalingi įrodymai vidaus drausminiams veiksmams, teisinei gynybai, draudimo reikalavimams ar komunikacijai su priežiūros institucijomis

2.2. Tai apima tiek faktinius, tiek įtariamus įvykius, susijusius su:

2.2.1. Duomenų nutekėjimu

2.2.2. Vidine grėsme arba netinkamu naudojimu

2.2.3. Saugumo pažeidimais (pvz., kenkimo programine įranga, neteisėta prieiga)

2.2.4. Klientų skundais, kuriems reikalingas skaitmeninis patvirtinimas

2.2.5. Priežiūros institucijų ar teisėsaugos užklausomis

3. Tikslai

3.1. Užtikrinti, kad visi įrodymai būtų renkami ir tvarkomi taip, kad būtų išlaikytas jų vientisumas, autentiškumas ir perdavimo grandinė.

3.2. Užkirsti kelią atsitiktiniam žurnalų, rinkmenų ar sistemų atvaizdų pakeitimui, ištrynimui ar netinkamam tvarkymui, kai jie gali būti reikalingi tyrimams.

3.3. Nustatyti nuoseklų ir audituojamą įrodymų valdymo procesą, atitinkantį teisinius ir reguliavimo lūkesčius (pvz., ES BDAR pranešimus apie pažeidimus, NIS2 atsekamumo reikalavimus).

3.4. Apibrėžti aiškius vaidmenis ir atsakomybes, kad saugumo incidentų metu būtų užtikrintas greitas, saugus ir teisės aktų reikalavimus atitinkantis įrodymų užfiksavimas.

3.5. Užtikrinti MVĮ lygmens pasirengimą skaitmeninei ekspertizei, kartu mažinant sudėtingumą ir netrikdant kasdienės veiklos.

4. Vaidmenys ir atsakomybės

4.1. Bendrovės vadovas (GM)

4.1.1. Tvirtina visus formalius tyrimus, kuriems reikalingas įrodymų rinkimas.

4.1.2. Peržiūri ir tvirtina incidentų ataskaitas, susijusias su galimais teisiniais ar drausminiais veiksmais.

4.1.3. Sprendžia, ar būtina informuoti išorės teisinį konsultantą ar priežiūros institucijas.

4.1.4. Užtikrina, kad politika būtų reguliariai peržiūrima ir atnaujinama.

4.2. IT paslaugų teikėjas / sistemų administratorius

4.2.1. Renka ir išsaugo skaitmeninius įrodymus laikydamasis saugių procedūrų.

4.2.2. Dokumentuoja laiko žymas, sistemos duomenis ir atliktus tvarkymo veiksmus.

4.2.3. Užtikrina, kad visa surinkta medžiaga būtų saugoma apsaugotoje vietoje.

4.2.4. Prireikus padeda atlikti skaitmeninės ekspertizės analizę.

[... 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 peržiūra

9.1.1. Ši politika ne rečiau kaip kartą per 12 mėnesių turi būti peržiūrima bendrovės vadovo (GM), siekiant patvirtinti:

9.1.1.1. Atitiktį ISO/IEC 27001 A priedo kontrolės priemonėms

9.1.1.2. Nuolatinį aktualumą esamoms skaitmeninėms platformoms ir IT paslaugoms

9.1.1.3. Žurnalų tvarkymo, įrodymų saugojimo ir pasirengimo skaitmeninei ekspertizei procedūrų pakankamumą

9.2. Įvykiai, sukeliantys politikos peržiūrą

9.2.1. Politika taip pat turi būti peržiūrima ir atnaujinama po:

9.2.1.1. Bet kokio reikšmingo incidento, kuriam reikėjo rinkti įrodymus

9.2.1.2. Nesėkmingo audito ar priežiūros institucijos užklausos, kai buvo suabejota įrodymų vientisumu

9.2.1.3. Naujų įrankių ar procedūrų, skirtų reagavimui į incidentus ar sistemų stebėsenai, įdiegimo

9.2.1.4. Teisės aktų pakeitimų (pvz., atnaujintų ES BDAR ar NIS2 gairių)

9.3. Pakeitimų tvirtinimas ir paskirstymas

9.3.1. Visi pakeitimai turi būti peržiūrėti ir patvirtinti GM.

9.3.2. Atnaujinta versija turi būti pateikta:

9.3.2.1. IT paslaugų teikėjams ir konsultantams, dalyvaujantiems tyrimuose

9.3.2.2. Visiems darbuotojams, atsakingiems už sistemų administravimą

9.3.3. Atnaujinta kopija turi būti saugoma bendrovės politikų archyve ir, pareikalavus, pateikiama auditoriams.

10. Susijusios politikos ir sąsajos

10.1. Ši politika yra susijusi su šiomis MVĮ pritaikytomis politikomis:

10.1.1. P2S – Valdysenos vaidmenų ir atsakomybių politika: nustato įgaliojimus incidentų tyrimams, sprendimams dėl įrodymų ir jų perdavimui teisiniam vertinimui.

10.1.2. P4S – Prieigos kontrolės politika: užtikrina, kad tyrimų metu prie jautrių sistemų ir žurnalų galėtų prieiti tik įgalioti asmenys.

10.1.3. P22S – Žurnalų tvarkymo ir stebėsenos politika: nustato pirminius duomenis, naudojamus kaip skaitmeninės ekspertizės įrodymai, ir apibrėžia saugojimo terminų, prieigos kontrolės bei žurnalų tvarkymo reikalavimus.

10.1.4. P30S – Reagavimo į incidentus politika: nustato poreikį rinkti įrodymus ir apibrėžia operacinę eigą, vedančią į skaitmeninės ekspertizės įrodymų išsaugojimą.

10.1.5. P17S – Duomenų apsaugos ir privatumo politika: užtikrina, kad visi kaip įrodymai surinkti asmens duomenys būtų tvarkomi teisėtai pagal ES BDAR ir susijusius teisės aktus.

10.2. Šios politikos kartu padeda užtikrinti teisinį pagrįstumą, tyrimo vientisumą ir pasirengimą ISO/IEC 27001:2022 auditui.

11. Pamatiniai standartai ir sistemos

11.1. ISO/IEC 27001

11.1.1. 6.1 punktas – Rizika grindžiamas planavimas apima pasirengimą reagavimui ir įrodymų procedūras.

11.1.2. 6.3 punktas – Palaiko gerinimo veiksmus, grindžiamus iš incidentų gautais įrodymais.

11.1.3. 8.1 punktas – Reikalauja operacinių kontrolės priemonių įrodymų vientisumui užtikrinti.

11.2. ISO/IEC 27002

11.2.1. Kontrolės priemonės 5.24–5.27 – Nustato saugų tvarkymą, peržiūras po incidentų ir įrodymais grindžiamą tobulinimą.

11.3. ISO/IEC 27035-3

11.3.1. 6.3, 6.4 ir 7.3 punktai – Užtikrina tinkamą planavimą, teisėtą rinkimą ir saugų skaitmeninių įrodymų tvarkymą reagavimo į incidentus metu, įskaitant išsaugojimą ir perdavimo grandinės dokumentavimą.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 ir AU-12 užtikrina pasirengimą skaitmeninei ekspertizei, audito žurnalų apsaugą ir veiksmingą įrodymų rinkimo integravimą į reagavimo į incidentus gyvavimo ciklą.

11.5. NIST SP 800-86

11.5.1. Apibrėžia gerąją praktiką skaitmeninių įrodymų gavimui, analizei ir apsaugai reagavimo į incidentus metu.

11.6. ES BDAR

11.6.1. 33–34 straipsniai – Reikalauja incidentų ir įrodymų dokumentavimo bei atsekamumo, kai pranešama apie asmens duomenų saugumo pažeidimus.

11.7. NIS2 direktyva (2022/2555)

11.7.1. 23 straipsnis – Reikalauja atsekamo incidentų pranešimo ir saugaus įrodymų tvarkymo esminiams ir svarbiems subjektams.

11.8. DORA reglamentas

11.8.1. 17 straipsnio 1 dalis – Užtikrina, kad su IRT susijusių incidentų įrodymai būtų renkami ir saugomi taip, kad palaikytų skaitmeninės ekspertizės tyrimus.

11.8.2. 17 straipsnio 2 dalis – Reikalauja, kad finansų subjektai išlaikytų visus susijusius duomenis ir žurnalus, susijusius su saugumo įvykiais, laikydamiesi skaitmeninės ekspertizės patikimumo ir reguliavimo užklausų reikalavimų.

11.9. COBIT 2019

11.9.1. DSS05.06 – Incidentų stebėsena, aptikimas ir pranešimas: pabrėžia patikimą žurnalų tvarkymą tyrimo palaikymui.

11.9.2. DSS05.07 – Incidentų tyrimas ir reagavimas: reikalauja struktūruoto įrodymų tvarkymo, kad būtų galima atlikti saugius ir audituojamus tyrimus.