					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P22S					Dokumento pavadinimas: **Žurnalų tvarkymo ir stebėsenos 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	8 skyrius	Operacinės kontrolės priemonės, įskaitant registravimą audito žurnaluose
ISO/IEC 27002:2022	Kontrolės priemonės 8.15, 8.16, 8.17	Įvykių registravimas, žurnalų apsauga ir stebėsena
NIST SP 800-53 Rev.5	AU-2–AU-12, SI-4	Audito žurnalų turinys / peržiūra, saugojimas, anomalijų nustatymas, įspėjimai
ES BDAR	5 straipsnio 1 dalies f punktas, 32, 33 straipsniai	Duomenų konfidencialumas / vientisumas, techninės priemonės ir pranešimas apie pažeidimą
ES NIS2 direktyva	21 straipsnio 2 dalies d punktas, 23 straipsnis	Žurnalavimo mechanizmai anomalijoms nustatyti ir pranešimas apie incidentus per 24 val.
ES DORA reglamentas	10, 15 straipsniai	Operacinis atsparumas, paslaugų teikėjų stebėsena / žurnalavimas
COBIT 2019	DSS01.03, DSS05.02	Veiklos atsekamumas ir apsauga taikant žurnalavimą / stebėseną

1. Tikslas

1.1 Ši politika nustato privalomas žurnalų tvarkymo ir stebėsenos kontrolės priemones, skirtas organizacijos IT sistemų saugumui, atskaitomybei ir operaciniam vientisumui užtikrinti.

1.2 Joje apibrėžiama, kokie įvykiai turi būti registruojami, kaip žurnalai saugomi, kaip jie peržiūrimi ir kokios yra darbuotojų bei paslaugų teikėjų atsakomybės.

1.3 Žurnalų tvarkymas ir stebėsena padeda užtikrinti grėsmių žvalgybą, atitiktį reglamentavimo reikalavimams, reagavimą į incidentus ir kriminalistinę analizę.

1.4 Ši politika padeda organizacijai įvykdyti ISO/IEC 27001 operacinių kontrolės priemonių reikalavimus ir palaiko nuolatinį pasirengimą auditui, klientų pasitikėjimą bei atitiktį ES BDAR, NIS2 direktyvos ir DORA reglamento reikalavimams.

2. Taikymo sritis

2.1 Ši politika taikoma visoms organizacijos sistemoms ir naudotojams, įskaitant:

2.1.1 darbo vietų kompiuterius, nešiojamuosius kompiuterius, serverius, ugniasienes, komutatorius, maršrutizatorius ir belaidės prieigos taškus;

2.1.2 debesijos paslaugas, naudojamas verslo veiklai (pvz., el. paštą, failų saugyklas, atsargines kopijas, bendradarbiavimo priemones);

2.1.3 žurnalavimo funkcijas antivirusinėje programinėje įrangoje, taikomosiose programose, operacinėse sistemose ir tinklo įrangoje;

2.1.4 visus darbuotojus, rangovus ir valdomų paslaugų teikėjus (MSP), kurie naudoja arba administruoja sistemas;

2.1.5 bet kurią vietą, kur naudojamos įmonės IT sistemos, įskaitant nuotolines, hibridines arba BYOD aplinkas.

2.2 Ši politika taip pat taikoma žurnalams, kuriuos generuoja trečiųjų šalių paslaugos, kai organizacija turi administratoriaus lygmens prieigą arba sutartyje nustatytą audito teisę.

3. Tikslai

3.1 Užtikrinti sistemų veiklos žurnalavimą, įskaitant autentifikavimą, konfigūracijos pakeitimus, prieigą prie jautrių duomenų ir saugumo įspėjimus.

3.2 Užtikrinti saugius ir tikslius žurnalus, kad būtų galima nustatyti politikos pažeidimus, sistemų klaidas ar neteisėtus veiksmus.

3.3 Sudaryti sąlygas operatyviai atlikti žurnalų peržiūrą incidentų, tyrimų ir auditų metu.

3.4 Užtikrinti laiko sinchronizavimą, kad būtų išlaikytas žurnalų duomenų vientisumas ir koreliacija.

3.5 Apsaugoti žurnalus nuo klastojimo, praradimo ar per ankstyvo ištrynimo.

3.6 Įvykdyti teisinius ir reglamentavimo įpareigojimus dėl sistemų atskaitomybės, atsekamumo ir reagavimo į pažeidimus.

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas (GM)

4.1.1 Tvirtina šią politiką ir užtikrina jos įgyvendinimą visose verslo sistemose.

4.1.2 Peržiūri didelio kritiškumo įspėjimus ir reikšmingas audito išvadas, apie kurias praneša IT arba duomenų apsaugos funkcija.

4.1.3 Tvirtina išimtis tais atvejais, kai žurnalavimo arba saugojimo terminų techniškai neįmanoma užtikrinti.

4.2 IT paslaugų teikėjas / vidinė IT funkcija

4.2.1 Įgyvendina ir konfigūruoja žurnalavimą operacinėse sistemose, tinklo įrenginiuose, antivirusinėse priemonėse ir pagrindinėse taikomosiose programose.

4.2.2 Užtikrina, kad žurnalai būtų saugomi, įtraukiami į atsargines kopijas ir apsaugoti nuo pakeitimų.

4.2.3 Peržiūri žurnalus pagal nustatytą grafiką ir tiria įtartiną arba neteisėtą veiklą.

4.2.4 Prižiūri įspėjimų sistemas, kurios fiksuoja anomalų elgesį arba įsibrovimo požymius.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Metinė peržiūra

9.1.1 Ši politika turi būti peržiūrima ne rečiau kaip kartą per metus Generalinio vadovo, padedant IT paslaugų teikėjui ir privatumo koordinatoriui.

9.2 Peržiūros prielaidos

9.2.1 Neplaninės peržiūros turi būti atliekamos reaguojant į:

9.2.1.1 su žurnalais susijusias vidaus arba išorės audito išvadas;

9.2.1.2 saugumo incidentus, kai žurnalų trūko, jie buvo sugadinti arba buvo nepakankami;

9.2.1.3 esminius IT infrastruktūros pokyčius (pvz., migraciją į debesijos žurnalavimo platformas);

9.2.1.4 teisinius arba reglamentavimo įpareigojimų atnaujinimus (pvz., ES BDAR, NIS2 direktyvą, DORA reglamentą).

9.3 Versijų kontrolė

9.3.1 Visi šios politikos pakeitimai turi būti registruojami nurodant versijos numerį, datą ir pakeitimų santrauką.

9.3.2 Ankstesnės versijos turi būti archyvuojamos ir saugomos mažiausiai 3 metus.

9.3.3 Atnaujinta politika turi būti komunikuojama paveiktoms suinteresuotosioms šalims, ypač turinčioms sistemos lygmens prieigą.

10. Susijusios politikos ir sąsajos

10.1 Ši politika tiesiogiai susijusi su toliau nurodytomis MVĮ informacijos saugumo politikomis ir jas papildo:

10.1.1 P17S – Duomenų apsaugos ir privatumo politika: užtikrina, kad žurnalų duomenys, kuriuose yra asmens informacijos, būtų valdomi užtikrinant vientisumą, saugojimą ir prieigos kontrolės priemones pagal ES BDAR reikalavimus.

10.1.2 P21S – Tinklo saugumo politika: sudaro pagrindą rinkti žurnalus, susijusius su ugniasienėmis, belaidžiu ryšiu, VPN ir segmentavimo stebėsena.

10.1.3 P24S – Saugaus kūrimo politika: užtikrina, kad taikomųjų programų žurnalai (pvz., prisijungimo bandymų, klaidų ir išimčių) būtų numatyti programinės įrangos projektavime ir eksploatavime.

10.1.4 P30S – Reagavimo į incidentus politika: remiasi tiksliais ir išsamiais žurnalų duomenimis, kad būtų galima aptikti, analizuoti ir valdyti informacijos saugumo įvykius.

10.1.5 P23S – Laiko sinchronizavimo politika: užtikrina nuoseklias ir atsekamas laiko žymas visose sistemose, leidžiančias koreliuoti žurnalus tyrimų metu.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8.1 punktas – reikalauja įgyvendinti operacines kontrolės priemones informacijos saugumo rizikai mažinti, įskaitant žurnalavimą.

11.2 ISO/IEC 27002

11.2.1 Kontrolės priemonė 8.15 – reikalauja įvykių registravimo, kad būtų palaikomas anomalijų nustatymas ir atskaitomybė.

11.2.2 Kontrolės priemonė 8.16 – reikalauja apsaugoti žurnalus nuo klastojimo ir neteisėtos prieigos.

11.2.3 Kontrolės priemonė 8.17 – reikalauja stebėti sistemas dėl neįprastos veiklos ir patvirtinti stebėsenos kontrolės priemonių veiksmingumą.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2–AU-12 – apima audito žurnalų turinį, peržiūrą, saugojimą ir automatizuotą įspėjimų generavimą.

11.3.2 SI-4 – reikalauja nustatyti sistemų anomalijas ir pranešti apie įtartinus įvykius.

11.4 ES BDAR

11.4.1 5 straipsnio 1 dalies f punktas – reikalauja užtikrinti asmens duomenų vientisumą ir konfidencialumą, įskaitant prieigos žurnalavimą.

11.4.2 32 straipsnis – nustato technines ir organizacines priemones saugumui užtikrinti, įskaitant žurnalavimą ir stebėseną.

11.4.3 33 straipsnis – reikalauja laiku pranešti apie pažeidimą, remiantis žurnalais, kurie leidžia atlikti pirminės priežasties analizę.

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies d punktas – reikalauja žurnalavimo mechanizmų, kurie nustato anomalijas ir padeda atliekant incidentų tyrimus.

11.5.2 23 straipsnis – įpareigoja pranešti apie incidentus per 24 valandas, o tai priklauso nuo tikslių ir laiku gaunamų žurnalų duomenų.

11.6 ES DORA reglamentas

11.6.1 10 straipsnis – reikalauja skaitmeninio operacinio atsparumo, įskaitant su IRT susijusių incidentų atsekamumą taikant žurnalavimą.

11.6.2 15 straipsnis – įpareigoja vykdyti paslaugų teikėjų stebėseną, įskaitant prieigą prie žurnalų ir jų peržiūros teises.

11.7 COBIT 2019

11.7.1 DSS01.03 – reikalauja sistemų veiklos atsekamumo taikant žurnalavimą ir stebėseną.

11.7.2 DSS05.02 – apibrėžia žurnalavimą kaip pagrindinę kontrolės priemonę apsaugai nuo kenkimo programinės įrangos ir kitos neteisėtos veiklos.