					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P22					Dokumento pavadinimas: **Žurnalų valdymo 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**

1. Tikslas

1.1 Šios politikos tikslas – nustatyti aiškius ir privalomus reikalavimus dėl žurnalų, kuriuose registruojami pagrindiniai sistemų ir saugumo įvykiai visoje organizacijos IT aplinkoje, generavimo, apsaugos, peržiūros ir analizės.

1.2 Žurnalų valdymas ir stebėsena yra būtini anomalijoms aptikti, reagavimui į grėsmes, kriminalistiniams tyrimams, pasirengimui auditui ir teisinei atitikčiai užtikrinti. Ši politika užtikrina, kad visi sistemų sugeneruoti įvykiai būtų tinkamai registruojami, saugomi ir koreliuojami, užtikrinant laiko sinchronizavimo tikslumą.

1.3 Ši politika būtina siekiant užtikrinti ISO/IEC 27001 8.1 punkto ir A priedo kontrolės priemonių 8.15 (registravimas audito žurnale), 8.16 (stebėsena) ir 8.17 (laikrodžių sinchronizavimas) įgyvendinimą ir yra tiesiogiai susieta su reguliaciniais įpareigojimais pagal ES BDAR, NIS2 direktyvą, DORA reglamentą ir COBIT 2019.

2. Taikymo sritis

2.1 Ši politika taikoma visoms sistemoms, paslaugoms ir aplinkoms, kuriose saugomi, tvarkomi ar perduodami duomenys, patenkantys į informacijos saugumo valdymo sistemos taikymo sritį, įskaitant:

2.1.1 vietinę infrastruktūrą, debesijos paslaugas (pvz., IaaS, PaaS, SaaS) ir hibridines aplinkas;

2.1.2 operacines sistemas, duomenų bazes, taikomąsias programas ir tinklo įrenginius;

2.1.3 saugumo sistemas, tokias kaip SIEM, ugniasienes, EDR platformas, VPN koncentratorius ir tapatybės teikėjus.

2.2 Į taikymo sritį įtraukiamos šios suinteresuotosios šalys:

2.2.1 vidaus naudotojai, turintys sistemos arba administratoriaus lygmens prieigą;

2.2.2 infrastruktūros ir IT operacijų darbuotojai;

2.2.3 saugumo operacijų centras ir grėsmių aptikimo komandos;

2.2.4 programinės įrangos kūrėjai ir taikomųjų programų savininkai;

2.2.5 trečiųjų šalių paslaugų teikėjai, valdantys žurnalus generuojančias sistemas.

3. Tikslai

3.1 Užtikrinti, kad visos kritinės sistemos generuotų saugumo įvykių žurnalus ir sistemų veiklos įrašus, kurie būtų saugomi laikantis reguliacinių, teisinių ir sutartinių reikalavimų.

3.2 Apibrėžti minimalius įvykių tipus ir žurnalų turinį, būtinus neteisėtai veiklai aptikti, naudotojų veiksmams atsekti ir kriminalistiniams tyrimams atlikti.

3.3 Įgyvendinti apsaugos priemones, užkertančias kelią žurnalų klastojimui, neteisėtam ištrynimui ar nekontroliuojamai prieigai prie žurnalų duomenų.

3.4 Įdiegti centralizuotas žurnalų valdymo ir perspėjimų sistemas (pvz., SIEM), skirtas įtartinai veiklai agreguoti, koreliuoti ir eskaluoti beveik realiuoju laiku.

3.5 Užtikrinti sistemų laikrodžių sinchronizavimą, kad būtų galima tiksliai koreliuoti įvykius tarp sistemų ir atlikti incidentų analizę.

3.6 Sudaryti sąlygas nuolatiniam tobulinimui ir atitikčiai, integruojant žurnalų stebėseną su audito, rizikos ir incidentų valdymo procesais.

4. Vaidmenys ir atsakomybės

4.1 Vyriausiasis informacijos saugumo pareigūnas

4.1.1 Yra šios politikos savininkas ir užtikrina jos suderinamumą su organizacijos rizikos apetitu, audito reikalavimais ir ISVS įpareigojimais.

4.1.2 Tvirtina registravimo apimtį reguliuojamoms arba didelės rizikos sistemoms ir vykdo atitikties ataskaitų priežiūrą.

4.2 Saugumo operacijų centro vadovas

4.2.1 Eksploatuoja ir prižiūri centralizuotas žurnalų valdymo platformas (pvz., SIEM).

4.2.2 Nustato žurnalų agregavimo taisykles, perspėjimų slenksčius ir incidentų triažo eskalavimo tvarką.

4.2.3 Peržiūri kasdienes ataskaitas ir užtikrina, kad anomalijos būtų analizuojamos, dokumentuojamos ir prireikus eskaluojamos.

[... 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 kasmet arba anksčiau, jei įvyksta:

9.1.1 reikšmingi sistemų architektūros arba žurnalų infrastruktūros pokyčiai (pvz., SIEM migracija);

9.1.2 žurnalavimui taikomų reguliacinių reikalavimų pakeitimai (pvz., NIS2 direktyvos, DORA reglamento žurnalavimo reikalavimai);

9.1.3 audito išvados arba paskesnių incidentų peržiūrų rezultatai;

9.1.4 naujai atsirandančios grėsmės, reikalaujančios sustiprintos stebėsenos (pvz., vidinės grėsmės, tiekimo grandinės kompromitavimas).

9.2 Peržiūros procesui turi vadovauti saugumo operacijų centro (SOC) vadovas, koordinuodamas veiklą su Vyriausiuoju informacijos saugumo pareigūnu, rizikos valdymo, atitikties ir IT infrastruktūros komandomis.

9.3 Patvirtinti pakeitimai turi būti valdomi taikant versijų kontrolę ISVS dokumentų kontrolės registre ir perduodami:

9.3.1 visoms suinteresuotosioms šalims, atsakingoms už žurnalavimo sistemų priežiūrą;

9.3.2 taikomųjų programų ir sistemų savininkams;

9.3.3 trečiųjų šalių teikėjams, turintiems telemetrijos arba SIEM integracijos pareigas.

9.4 Visos pakeistos ankstesnės versijos turi būti saugiai archyvuojamos, o prieiga prie jų turi būti ribojama tik autorizuotiems ISVS saugotojams audito ir teisiniais tikslais.

10. Susijusios politikos ir sąsajos

10.1 P1 – Informacijos saugumo politika. Nustato pagrindinį įsipareigojimą apsaugoti sistemas ir duomenis, o žurnalų valdymas ir stebėsena pagal ją veikia kaip esminės prevencinės ir reagavimo kontrolės priemonės.

10.2 P4 – Prieigos kontrolės politika. Užtikrina, kad privilegijuota prieiga, naudotojų prisijungimai ir autorizavimo įvykiai būtų registruojami žurnaluose ir stebimi dėl piktnaudžiavimo ar anomalios elgsenos.

10.3 P5 – Pakeitimų valdymo politika. Nustato prievolę registruoti sistemų pakeitimus, pataisų diegimą ir konfigūracijos atnaujinimus, kurie gali sukelti riziką arba lemti nesankcionuotus pakeitimus.

10.4 P21 – Tinklo saugumo politika. Reikalauja tinklo lygmens žurnalavimo (pvz., ugniasienių žurnalų, IDS / IPS perspėjimų, VPN veiklos) ir integracijos su SIEM, siekiant užtikrinti tinklo srauto anomalijų matomumą ir perimetro apsaugą.

10.5 P23 – Laiko sinchronizavimo politika. Užtikrina laikrodžių suderinamumą tarp sistemų, kuris yra būtinas patikimam žurnalavimui ir saugumo įvykių koreliacijai keliose aplinkose.

10.6 P30 – Reagavimo į incidentus politika. Remiasi žurnalų duomenimis ir perspėjimų mechanizmais saugumo incidentams nustatyti, tirti ir valdyti, kartu išsaugant kriminalistinius artefaktus poincidentinei peržiūrai.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8.1 punktas – operacinis planavimas ir kontrolė: reikalauja taikyti kontrolės priemones operacijų stebėsenai ir apsaugai nuo neteisėtos prieigos bei netinkamo sistemų naudojimo.

11.2 ISO/IEC 27002:2022 – kontrolės priemonės 8.15, 8.16, 8.17

11.2.1 Apibrėžia išsamius žurnalavimo reikalavimus, įskaitant tai, kokie įvykiai turi būti registruojami, kaip apsaugoti ir analizuoti žurnalus bei kaip užtikrinti laiko žymų patikimumą visose sistemose.

11.3 NIST SP 800-53 5 red.

11.3.1 AU-2–AU-12: apima įvykių parinkimą, registravimą, apsaugą, audito peržiūrą, reagavimą į audito nesėkmes ir audito įrašų saugojimą.

11.3.2 SI-4 – sistemų stebėsena: reikalauja aktyvios sistemų stebėsenos su perspėjimais, grindžiamais anomaline veikla.

11.3.3 SC-45 – sistemų laiko sinchronizavimas: sustiprina laiko tikslumo reikalavimą įvykių atsekamumui ir incidentų koreliacijai.

11.4 ES BDAR (2016/679)

11.4.1 32 straipsnis – tvarkymo saugumas: reikalauja techninių kontrolės priemonių, tokių kaip žurnalavimas ir stebėsena, siekiant užtikrinti saugumą ir atskaitomybę, ypač prieigai prie asmens duomenų.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21 straipsnio 2 dalies e punktas: nustato prievolę taikyti įvykių registravimo ir stebėsenos sistemas, skirtas sparčiam saugumo incidentų aptikimui ir reagavimui.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 9 straipsnis – IRT rizikos valdymas: reikalauja mechanizmų anomalinei veiklai aptikti, incidentams registruoti ir kriminalistiniams duomenims saugoti.

11.6.2 11 straipsnis – IRT veiklos tęstinumo planų testavimas: pabrėžia stebėsenos tęstinumą ir žurnalų prieinamumo validavimą veiklos sutrikimų metu.

11.7 COBIT 2019

11.7.1 DSS01.05 – saugumo žurnalų valdymas: reikalauja įdiegti žurnalavimo galimybes visai kritinei infrastruktūrai.

11.7.2 DSS05.04 – saugumo įvykių stebėsena: nustato realiojo laiko žurnalų stebėseną ir analizę, skirtą įvykiams aptikti ir į juos reaguoti.

11.7.3 MEA03 – stebėti, vertinti ir vertinti atitiktį: reikalauja reguliarios žurnalavimo praktikos peržiūros ir suderinamumo su kontrolės priemonių tikslais.