					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P23					Dokumento pavadinimas: **Laiko sinchronizavimo 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	Punktas / straipsnis	Komentaras
ISO/IEC 27001:2022	8 punktas	-
ISO/IEC 27002:2022	Kontrolė 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
ES BDAR	32 straipsnis	-
ES NIS2 direktyva	21 straipsnio 2 dalies e punktas	-
ES DORA reglamentas	9, 10 straipsniai	-
COBIT 2019	DSS05.04, MEA	-

1. Tikslas

1.1 Šios politikos tikslas – užtikrinti, kad visose organizacijos sistemose, taikomosiose programose, įrenginiuose ir debesijos paslaugose būtų palaikomi nuoseklūs ir tikslūs laiko nustatymai, sinchronizuoti su paskirtais patikimais laiko šaltiniais.

1.2 Tikslus laiko sinchronizavimas yra būtinas patikimam žurnalų tvarkymui, saugiam ryšiui, audito atsekamumui, reagavimui į incidentus ir skaitmeninei kriminalistikai. Nesinchronizuotas laikas gali lemti nekoreliuojamus žurnalus, autentifikavimo klaidas ir neišsamų atitikties ataskaitų teikimą.

1.3 Ši politika įgyvendina ISO/IEC 27001 A priedo kontrolę 8.17 ir susijusių tarptautinių standartų reikalavimus, nustatydama laiko tikslumo užtikrinimo ir laikrodžio nuokrypio aptikimo principus visoje organizacijos IT aplinkoje.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 Visiems infrastruktūros komponentams, įskaitant serverius, darbo vietas, tinklo įrenginius, užkardas ir IoT sistemas

2.1.2 Virtualiosioms ir debesijos aplinkoms (pvz., AWS, Azure, Google Cloud)

2.1.3 Visoms sistemoms, dalyvaujančioms žurnalų tvarkyme, autentifikavime, operacijų apdorojime arba saugumo įvykių koreliacijoje

2.1.4 Vidaus darbuotojams, rangovams ir trečiųjų šalių paslaugų teikėjams, atsakingiems už laiko požiūriu jautrias sistemas

2.2 Ši politika visa apimtimi taikoma sistemoms, kurios generuoja arba naudoja įrašus su laiko žyma, pavyzdžiui, žurnalų įrašus, įspėjimus, naudotojų veiklos įrašus ar skaitmeninės kriminalistikos įrodymus.

3. Tikslai

3.1 Nustatyti nuoseklią ir centralizuotą laiko sinchronizavimo architektūrą, naudojančią patvirtintus NTP šaltinius arba lygiaverčius sprendimus.

3.2 Užtikrinti, kad visų sistemų laikrodžiai būtų sinchronizuojami nustatytais intervalais, o bet koks nuokrypis būtų aptinkamas ir šalinamas automatiškai arba su minimalia intervencija.

3.3 Užtikrinti laikrodžių tikslumą hibridinėse aplinkose, vietinėje infrastruktūroje ir debesijos aplinkose, siekiant sudaryti sąlygas:

3.3.1 Patikimai įvykių koreliacijai ir reagavimui į incidentus

3.3.2 Atitikčiai teisės aktų ir standartų reikalavimams, tokiems kaip ISO 27001, ES BDAR, NIS2 direktyva ir DORA reglamentas

3.3.3 Apsaugai nuo pakartojimo atakų ir su laiku susijusių autentifikavimo nesėkmių

3.4 Nustatyti aiškius vaidmenis, išimčių valdymo procedūras ir audito mechanizmus, kad būtų užtikrintas šios politikos taikymas.

3.5 Užtikrinti, kad su laiku susijusios anomalijos būtų registruojamos žurnaluose, generuotų įspėjimus ir būtų eskaluojamos, kai viršijami leistini nuokrypiai.

4. Vaidmenys ir atsakomybės

4.1 Informacijos saugumo vadovas (CISO)

4.1.1 Valdo šią politiką ir užtikrina jos suderinamumą su ISVS operacinėmis kontrolės priemonėmis ir teisės aktų reikalavimais.

4.1.2 Tvirtina įmonės lygmens laiko šaltinių parinkimą ir patvirtina laiko sinchronizavimo ataskaitų teikimo procesus.

4.2 Infrastruktūros paslaugų vadovas / tinklų inžinerijos vadovas

4.2.1 Prižiūri organizacijos pirminius ir antrinius NTP serverius arba paskirtą laiko šaltinių konfigūraciją.

4.2.2 Užtikrina, kad visi prie tinklo prijungti įrenginiai ir virtualiosios instancijos sinchronizuotų laiką tinkamais intervalais.

4.2.3 Vykdo laiko sinchronizavimo žurnalų, laikrodžio nuokrypio įspėjimų ir sutrikimų būsenų stebėseną.

[... 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 susiklosto bent viena iš šių sąlygų:

9.1.1 Aptinkami su laiku susiję išnaudojimo atvejai arba žurnalų tvarkymo nesėkmės

9.1.2 Keičiama pagrindinė laiko infrastruktūra (pvz., nauji įmonės NTP serveriai arba protokolų atnaujinimai)

9.1.3 Nustatomi debesijos platformų laiko nuokrypio neatitikimai arba regioninių paslaugų pokyčiai

9.1.4 Po incidento nustatomos audito išvados, identifikuojančios laiko nesuderinamumą kaip prisidedantį veiksnį

9.2 Peržiūrą turi koordinuoti infrastruktūros vadovas, privalomai įtraukiant SOC, taikomųjų programų saugumo ir atitikties funkcijų atstovus.

9.3 Pakeitimai turi būti dokumentuojami ISVS dokumentų registre ir komunikuojami paveiktoms vidaus bei trečiųjų šalių suinteresuotosioms šalims.

9.4 Istorinės politikos versijos turi būti saugiai archyvuojamos, valdomos taikant versijų kontrolę ir pateikiamos atitikties arba teisinių auditų užklausoms.

10. Susijusios politikos ir sąsajos

10.1 P1 – Informacijos saugumo politika. Nustato bendrąjį reikalavimą užtikrinti visų informacinių sistemų vientisumą ir atsekamumą, kuriam laiko tikslumas yra esminė prielaida.

10.2 P5 – Pakeitimų valdymo politika. Reglamentuoja sistemų konfigūracijų pakeitimus, įskaitant laiko šaltinių koregavimą, užtikrindama tinkamą dokumentavimą, testavimą ir grąžinimo į ankstesnę būseną planus.

10.3 P22 – Žurnalų tvarkymo ir stebėsenos politika. Tiesiogiai priklauso nuo sinchronizuoto laiko, kad būtų užtikrintas įvykių nuoseklumas, žurnalų koreliacija ir incidentų tyrimo vientisumas skirtingose sistemose.

10.4 P30 – Reagavimo į incidentus politika. Remiasi tiksliomis laiko žymomis skaitmeninės kriminalistikos tyrimams, incidentų chronologijai ir perdavimo grandinės dokumentacijai. Netikslus laikas mažina incidentų ataskaitų patikimumą.

10.5 P20 – Galinių įrenginių apsaugos / apsaugos nuo kenkimo programinės įrangos politika. Reikalauja laiko požiūriu tikslaus įspėjimų generavimo ir elgsenos analizės, kad būtų galima nustatyti kenkimo programinės įrangos plitimą, šoninį judėjimą ir prieigos anomalijas.

10.6 P6 – Rizikos valdymo politika. Apibrėžia desinchronizaciją kaip galimą operacinę ir skaitmeninės kriminalistikos riziką bei reikalauja šioje politikoje nustatytų kontrolės priemonių poveikiui mažinti.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8.1 punktas – operacinis planavimas ir kontrolė: reikalauja integruoti tikslias techninės kontrolės priemones, pavyzdžiui, sinchronizuotus sistemų laikrodžius, kad būtų užtikrintas patikimas operacinis vykdymas.

11.2 ISO/IEC 27002:2022 – Kontrolė 8

11.2.1 Pabrėžia laikrodžio tikslumo svarbą ir reikalauja organizacinio sistemų laiko nuoseklumo, kad būtų galima palyginti žurnalus, atlikti tyrimus ir patvirtinti saugias operacijas.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – sistemų laiko sinchronizavimas: reikalauja naudoti patikimą šaltinį laiko sinchronizavimui visuose sistemos ribose esančiuose komponentuose.

11.3.2 AU-8 – laiko žymos: užtikrina, kad įvykiams būtų tiksliai priskirtos laiko žymos, ir sudaro sąlygas atsekamumui audito ir reagavimo į incidentus tikslais.

11.4 ES BDAR (2016/679)

11.4.1 32 straipsnis – Tvarkymo saugumas: nors aiškiai nemini laiko, reikalauja taikyti tinkamas techninės priemones, įskaitant audito pėdsakus ir žurnalus, kurių galiojimas ir vientisumas tiesiogiai priklauso nuo sinchronizuotų laiko žymų.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21 straipsnio 2 dalies e punktas: reikalauja žurnalų tvarkymo ir aptikimo pajėgumų, kurie suponuoja tikslų laiko sinchronizavimą tarp sistemų koreliacijai ir savalaikiam reagavimui.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 9 straipsnis – IRT rizikos valdymas: reikalauja tikslios sistemų telemetrijos rizikos stebėsenai ir anomalijų aptikimui, o tai priklauso nuo tikslaus laikrodžių sinchronizavimo.

11.6.2 10 straipsnis – IRT veiklos tęstinumas: nustato kontrolės priemones, užtikrinančias sistemų vientisumą sutrikimų metu, įskaitant laiko požiūriu suderintus įvykių įrašus.

11.7 COBIT 2019

11.7.1 DSS05.04 – saugumo įvykių stebėsena: reikalauja laiko žymų vientisumo veiksmingai žurnalų analizei ir grėsmių aptikimui.

11.7.2 MEA03 – atitikties stebėsena, vertinimas ir vertinimas: laiko sinchronizavimas palaiko tikslų atitikties auditą ir ataskaitų teikimo ciklus.