

				Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P23S				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

<p>Teisinis pranešimas (autorių teisės ir naudojimo apribojimai) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>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.</p> <p>Neautorizuotas naudojimas yra griežtai draudžiamas ir gali užtraukti teisinius veiksmus.</p> <p>Dėl licencijavimo kreipkitės: info@clarysec.com</p>

Suderinta su standartais ir reglamentais

Standartas / reglamentas	Skyrius / straipsnis	Komentaras
ISO/IEC 27001:2022	8 skyrius	Susiję kontrolės priemonių reikalavimai
ISO/IEC 27002:2022	Kontrolė 8	Sinchronizuotas sistemų veikimas
NIST SP 800-53 Rev.5	SC-45, AU-8	Patikimas NTP ir tikslios žurnalų laiko žymos
ES BDAR	5 straipsnio 1 dalies d punktas, 32 straipsnis	Tikslumas, atskaitomybė ir asmens duomenų vientisumas naudojant sinchronizuotas laiko žymas
NIS2 direktyva	21 straipsnio 2 dalies d punktas	Stebėsenos ir aptikimo galimybės, grindžiamos sinchronizuotais žurnalais
DORA reglamentas	10, 15 straipsniai	Veiklos atsparumas ir tikslūs techniniai įrašai
COBIT 2019	DSS05.02, MEA03	Laiko žymomis pažymėti įvykiai ir įrodymais grindžiama stebėseną

1. Tikslas

1.1 Ši politika nustato privalomas kontrolės priemones, skirtas užtikrinti tikslų ir sinchronizuotą laiką visose sistemose, kurios saugo, perduoda arba tvarko organizacijos duomenis.

1.2 Laiko sinchronizavimas yra būtinas siekiant užtikrinti sistemų žurnalų atsekamumą, tikslų saugumo incidentų susiejimą ir patikimą įrodymų naudojimą skaitmeninės kriminalistikos analizės ar teisinio vertinimo metu.

1.3 Organizacija taiko automatinį laiko sinchronizavimą kaip bazinį reikalavimą, siekdama užtikrinti audito vientisumą, reagavimą į incidentus ir atitiktį pagal ISO 27001, ES BDAR, DORA reglamentą ir NIS2 direktyvą.

1.4 Ši politika užtikrina, kad visose sistemose būtų naudojami patikimi laiko šaltiniai, būtų užkirstas kelias rankiniam laiko nustatymų keitimui ir būtų reikalaujama laiku ištaisyti laikrodžio nuokrypį.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 Visoms įmonei priklausančioms sistemoms ir įrenginiams, įskaitant serverius, stalinius kompiuterius, nešiojamuosius kompiuterius, mobiliuosius įrenginius, ugniasienes, maršrutizatorius ir virtualiąsias mašinas

2.1.2 Nuotolinei ir debesijos infrastruktūrai, naudojamai veikloje (pvz., AWS, Microsoft 365, SaaS platformoms)

2.1.3 Sistemoms, kurios generuoja ar saugo įvykių žurnalus, autentifikavimo įrašus ar audito pėdsakus

2.1.4 Visiems darbuotojams, rangovams, tiekėjams ar IT pagalbos paslaugų teikėjams, atsakingiems už šių sistemų konfigūravimą ar priežiūrą

2.2 Politika taip pat taikoma BYOD galiniams įrenginiams, naudojamiems prieigai prie verslo sistemų, jei šie galiniai įrenginiai saugo arba generuoja auditui reikšmingus duomenis.

3. Tikslai

- 3.1 Užtikrinti, kad visos kritinės svarbos sistemos automatiškai sinchronizuotų laiką naudodamos patikimus tinklo laiko protokolo (NTP) serverius arba lygiaverčius debesijos paslaugų teikėjo mechanizmus
- 3.2 Užkirsti kelią laiko neatitikimams, kurie galėtų pakenkti sistemų žurnalų patikimumui ar susiejamumui auditų ar saugumo tyrimų metu
- 3.3 Sudaryti sąlygas laiku aptikti ir ištaisyti laiko nuokrypį, viršijantį priimtinius slenksčius
- 3.4 Užtikrinti nuoseklų laiko žymų taikymą visose aplinkose (vietinėje infrastruktūroje, debesijoje ir nuotolinėje aplinkoje)
- 3.5 Atitikti techninius ir teisinius vientisumo, atsekamumo ir nepaneigiamumo reikalavimus, taikomus įrašams ir įvykiams

4. Vaidmenys ir atsakomybės

4.1 Generalinis direktorius

- 4.1.1 Tvirtina šią politiką ir užtikrina jos laikymąsi visoje organizacijoje
- 4.1.2 Prižiūri periodines sistemų lygmens laiko tikslumo peržiūras ir įgyvendinimo spragų vertinimą
- 4.1.3 Tvirtina automatinio laiko sinchronizavimo išimtis, jei jos yra pagrįstos ir dokumentuotos

4.2 IT pagalbos paslaugų teikėjas / vidaus IT funkcija

- 4.2.1 Konfigūruoja laiko sinchronizavimą visoms įmonei priklausančioms ar jos valdomoms sistemoms
- 4.2.2 Tikrina, ar kasdienis arba suplanuotas sinchronizavimas veikia tinkamai
- 4.2.3 Tiria ir šalina laiko nuokrypio incidentus, sinchronizavimo nesėkmes ar NTP prieigos problemas
- 4.2.4 Dokumentuoja laiko sinchronizavimo būseną kaip mėnesinių sistemų būklės patikrų dalį

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Planinė peržiūra

- 9.1.1 Šią politiką kasmet turi peržiūrėti generalinis direktorius, IT pagalbos paslaugų teikėjas ir privatumo koordinatorius
- 9.1.2 Peržiūros metu turi būti įvertinti visi žurnalai ir laiko sinchronizavimo atitikties būsenos ataskaitos

9.2 Atnaujinimai pagal suveikimo sąlygas

9.2.1 Ši politika turi būti atnaujinta, jeigu:

- 9.2.1.1 Sistemos sutrikimas sukelia reikšmingą laiko nuokrypį
- 9.2.1.2 Auditas nustato laiko sinchronizavimo trūkumus
- 9.2.1.3 Organizacija pradeda naudoti naujas debesijos, hibridines arba virtualizavimo aplinkas
- 9.2.1.4 Teisiniai ar reglamentavimo pokyčiai nustato naujus laiko vientisumo reikalavimus

9.3 Versijų kontrolė ir komunikacija

- 9.3.1 Visi atnaujinimai turi būti valdomi taikant versijų kontrolę ir datuojami
- 9.3.2 Apie esminius pakeitimus turi būti informuojamas visas techninis personalas
- 9.3.3 Ankstesnės versijos turi būti saugomos 3 metus audito poreikiams pagrįsti

10. Susijusios politikos ir sąsajos

10.1 Ši politika turi būti taikoma kartu su šiomis MVĮ politikomis:

- 10.1.1 P22S – Žurnalų tvarkymo ir stebėsenos politika: užtikrina nuoseklų laiko žymų taikymą žurnaluose, kad būtų užtikrintas atsekamumas ir skaitmeninės kriminalistikos susiejamumas.

10.1.2 P30S – Reagavimo į incidentus politika: remiasi tiksliais laiko žymomis siekiant atkurti incidentų eigą, nustatyti laiko seką ir pagrįsti sprendimus dėl pranešimų.

10.1.3 P17S – Duomenų apsaugos ir privatumo politika: užtikrina, kad priegos žurnalai ir su asmens duomenimis susijusio duomenų tvarkymo laiko seka būtų tikslūs ir pagrindžiami pagal ES BDAR.

10.1.4 P12S – Turto valdymo politika: padeda identifikuoti sistemas, kurioms reikalingas sinchronizavimas, ypač mobiliuosius ir nuotolinius įrenginius.

10.1.5 P26S – Trečiųjų šalių ir tiekėjų saugumo politika: užtikrina, kad tiekėjai, kurie organizacijos vardu pasiekia ar registruoja duomenis, pagal sutartis taikytų sinchronizuoto laiko praktiką.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001:

11.1.1 8.1 skyrius – reikalauja įgyvendinti saugiai veiklai būtinas kontrolės priemones, įskaitant žurnalų tvarkymą ir laiko žymų taikymą.

11.2 ISO/IEC 27002:

11.2.1 Kontrolė 8.17 – rekomenduoja sinchronizuotą laiką visoms sistemoms, kurios generuoja žurnalus arba sąveikauja su kitomis sistemomis.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – reikalauja naudoti vidinius arba išorinius laiko šaltinius žurnalų laiko žymų tikslumui užtikrinti.

11.3.2 SC-45 – nurodo naudoti patikimus NTP šaltinius ir užkirsti kelią rankiniam laiko keitimui kritinėse sistemose.

11.4 ES BDAR:

11.4.1 5 straipsnio 1 dalies d punktas – reikalauja tikslumo ir atskaitomybės tvarkant asmens duomenis, tai užtikrinant sinchronizuotomis laiko žymomis.

11.4.2 32 straipsnis – reikalauja saugumo priemonių, užtikrinančių duomenų vientisumą, įskaitant nuoseklius žurnalų laiko intervalus.

11.5 NIS2 direktyva:

11.5.1 21 straipsnio 2 dalies d punktas – reikalauja stebėsenos ir aptikimo galimybių, grindžiamų sinchronizuotais sistemų žurnalais.

11.6 DORA reglamentas:

11.6.1 10 straipsnis – reikalauja veiklos atsparumo, įskaitant atsekamus ir laiko žymomis pažymėtus IRT incidentų žurnalus.

11.6.2 15 straipsnis – reikalauja, kad paslaugų teikėjai tvarkytų tikslus techninius įrašus, įskaitant laiko žymomis pažymėtą audito pėdsaką.

11.7 COBIT 2019:

11.7.1 DSS05.02 – pabrėžia laiko žymų vientisumo svarbą aptinkant įvykius ir į juos reaguojant.

11.7.2 MEA03.01 – reikalauja veiksmingumo stebėsenos, grindžiamos įrodymais, kurią palaiko tikslūs laiko atžvilgiu sinchronizuoti duomenys.