

				Daħnal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P23S				Titlu tad-dokument: Politika tas-Sinkronizzazzjoni tal-Ħin							
Verżjoni: 1.0		Data tad-dħul fis-seħħ: 01.01.2025		Sid tad-dokument:							
X	Politika		Standard		Proċedura		Formola		Reġistru		Oħra

Storja tar-reviżjonijiet				
Numru tar-reviżjoni	Data tar-reviżjoni	Bidliet	Ivvedut minn	Sid tal-proċess

Approvazzjonijiet			
Isem	Pożizzjoni	Data	Firma

Avviż legali (drittijiet tal-awtur u restrizzjonijiet fuq l-użu)
(C) 2025 Clarysec LLC. All rights reserved.

Dan id-dokument huwa proprjetà intellettuali ta' Clarysec LLC. L-ebda parti minn dan id-dokument ma tista' tiġi kkupjata, użata mill-ġdid, distribwita jew modifikata għal skopijiet kummerċjali jew ta' implimentazzjoni mingħajr awtorizzazzjoni espliċita minn qabel bil-miktub.

L-użu mhux awtorizzat huwa strettament ipprobit u jista' jwassal għal azzjoni legali.

Għal-liċenzjar, ikkuntattja: info@clarysec.com

Allinjata ma' standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	Rekwiżiti ta' kontrolli rilevanti
ISO/IEC 27002:2022	Kontroll 8	Tħaddim sinkronizzat tas-sistema
NIST SP 800-53 Rev.5	SC-45, AU-8	NTP affidabbli u preċiżjoni tat-timestamps fil-logs
GDPR tal-UE	Artikoli 5(1)(d), 32	Preċiżjoni, accountability u integrità tad-data personali permezz ta' timestamps sinkronizzati
Direttiva NIS2 tal-UE	Artikolu 21(2)(d)	Kapaċitajiet ta' monitoraġġ u skoperta appoġġjati minn logs sinkronizzati
DORA tal-UE	Artikoli 10, 15	Reżiljenza operattiva u reġistri tekniċi preċiżi
COBIT 2019	DSS05.02, MEA03	Avvenimenti b'timestamp u monitoraġġ ibbażat fuq l-evidenza

Għan

1.1 Din il-politika tistabbilixxi kontrolli obbligatori biex jinżamm ħin preċiż u sinkronizzat fis-sistemi kollha li jaħżnu, jittrasmettu jew jipproċessaw id-data tal-organizzazzjoni.

1.2 Is-sinkronizzazzjoni tal-ħin hija essenzjali biex tiżgura li l-logs tas-sistema jkunu traċċabbli, li l-incidenti tas-sigurtà tal-informazzjoni jkunu jistgħu jiġu kkorrelati b'mod preċiż, u li l-evidenza tkun tista' tintuża waqt analiżi forensika jew rieżami legali.

1.3 L-organizzazzjoni teħtieġ sinkronizzazzjoni awtomatizzata tal-ħin bħala rekwiżit fundamentali għall-integrità tal-awditjar, ir-rispons għall-incidenti u l-konformità regolatorja skont ISO 27001, GDPR, DORA u NIS2.

1.4 Din il-politika tiżgura li s-sistemi kollha jużaw sorsi tal-ħin fdati, tipprevjeni tibdil manwali fl-impostazzjonijiet tal-ħin, u tirrikjedi korrezzjoni f'waqtha ta' kull devjazzjoni tal-arloġġ.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 Is-sistemi u l-apparati kollha proprjetà tal-kumpanija, inklużi servers, desktops, laptops, apparati mobbli, firewalls, routers u magni virtwali

2.1.2 Infrastruttura remota u sistemi ospitati fil-cloud użati fl-operazzjonijiet (eż. AWS, Microsoft 365, pjattaformi SaaS)

2.1.3 Sistemi li jiġġeneraw jew jaħżnu logs ta' avvenimenti, reġistri ta' awtentikazzjoni jew traċċi ta' awditjar

2.1.4 Kull impjegat, kuntrattur, fornitur jew fornitur ta' appoġġ tal-IT responsabbli għall-konfigurazzjoni jew il-manutenzjoni ta' dawn is-sistemi

2.2 Il-politika tapplika wkoll għal endpoints BYOD użati biex jaċċessaw sistemi tan-negozju, sakemm dawn l-endpoints jaħżnu jew jiġġeneraw data rilevanti għall-awditjar.

3. Objettivi

- 3.1 Jiġi żgurat li s-sistemi kritiċi kollha jissinkronizzaw il-ħin awtomatikament billi jużaw servers fdati tan-Network Time Protocol (NTP) jew mekkanizmi ekwivalenti tal-fornitur tal-cloud
- 3.2 Jiġu evitati diskrepanzi fil-ħin li jistgħu jdgħajfu l-affidabbiltà jew il-korrelazzjoni tal-logs tas-sistema waqt awditi jew investigazzjonijiet ta' sigurtà
- 3.3 Jippermetti s-sejbien u l-korrezzjoni f'waqthom ta' devjazzjoni tal-ħin lil hinn mil-limiti aċċettabbli
- 3.4 Tinżamm konsistenza fit-timestamps bejn l-ambjenti kollha (fuq il-post, cloud u remot)
- 3.5 Jiġu ssodisfati r-rekwiżiti tekniċi u legali għall-integrità, it-traċċabbiltà u n-nuqqas ta' ċaħda tar-reġistri u l-avvenimenti

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

- 4.1.1 Japprova din il-politika u jiżgura l-konformità organizzattiva
- 4.1.2 Jeżerċita sorveljanza fuq rieżamijiet perjodiċi tal-preċiżjoni tal-ħin fil-livell tas-sistema u fuq kwalunkwe lakuna fl-implimentazzjoni
- 4.1.3 Japprova eċċezzjonijiet għas-sinkronizzazzjoni awtomatizzata tal-ħin fejn dawn ikunu ġustifikati u dokumentati

4.2 Fornitur ta' Appoġġ tal-IT / Rwol Intern tal-IT

- 4.2.1 Jikkonfigura s-sinkronizzazzjoni tal-ħin għas-sistemi kollha proprjetà tal-kumpanija jew immaniġġjati minnha
- 4.2.2 Jivverifika li s-sinkronizzazzjoni ta' kuljum jew skedata tkun qed taħdem kif suppost
- 4.2.3 Jinvestiga u jwettaq rimedju għal avvenimenti ta' devjazzjoni tal-ħin, fallimenti ta' sinkronizzazzjoni jew kwistjonijiet ta' aċċess għall-NTP
- 4.2.4 Jiddokumenta l-istatus tas-sinkronizzazzjoni tal-ħin bħala parti mill-kontrolli mensili tas-saħħa tas-sistema

[... Is-sezzjonijiet 4.3–8 mhumiex inklużi f'dan il-preview. Ixtri d-dokument sħiħ biex taċċessa l-kontenut kollu. ...]

9. Rekwiżiti għar-rieżami u l-aġġornament

9.1 Rieżami skedat

- 9.1.1 Din il-politika għandha tiġi rieżaminata kull sena mill-Maniġer Ġenerali, il-Fornitur ta' Appoġġ tal-IT u l-Koordinatur tal-Privatezza
- 9.1.2 Il-logs kollha u r-rapporti dwar l-istatus tal-konformità mas-sinkronizzazzjoni tal-ħin għandhom jiġu kkunsidrati waqt ir-rieżami

9.2 Aġġornamenti bbażati fuq skattaturi

9.2.1 Din il-politika għandha tiġi aġġornata jekk:

- 9.2.1.1 Falliment ta' sistema jirriżulta f'devjazzjoni sinifikanti tal-ħin
- 9.2.1.2 Awditu jiżvela nuqqasijiet fis-sinkronizzazzjoni tal-ħin
- 9.2.1.3 L-organizzazzjoni tadotta ambjenti ġodda cloud, ibridi jew ta' virtualizzazzjoni
- 9.2.1.4 Bidliet legali jew regolatorji jintroduċu rekwiżiti ġodda għall-integrità tal-ħin

9.3 Kontroll tal-verżjoni u komunikazzjoni

- 9.3.1 L-aġġornamenti kollha għandhom ikunu taħt kontroll tal-verżjoni u datati
- 9.3.2 Bidliet materjali għandhom jiġu kkomunikati lill-persunal tekniku kollu
- 9.3.3 Verżjonijiet preċedenti għandhom jinżammu għal 3 snin biex jappoġġjaw l-awditjar

10. Politiki relatati u rabtiet

10.1 Din il-politika għandha tiġi applikata flimkien mal-politiki SME li ġejjin:

10.1.1 P22S – Politika tal-Illoggjar u l-Monitoraġġ: Tiżgura timestamping konsistenti bejn il-logs għat-traċċabbiltà u l-korrelazzjoni forensika.

10.1.2 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiddependi fuq il-preċiżjoni tat-timestamp biex tirrikostitwixxi l-inċidenti, tiddefinixxi l-linji taż-żmien u tappoġġja deċiżjonijiet ta' notifika.

10.1.3 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tiżgura li l-logs tal-aċċess u l-linji taż-żmien tal-immaniġġjar tad-data li jinvolvu data personali jkunu preċiżi u difendibbli skont il-GDPR.

10.1.4 P12S – Politika tal-Ġestjoni tal-Assi: Tappoġġja l-identifikazzjoni ta' sistemi li jeħtieġu sinkronizzazzjoni, b'mod partikolari apparati mobbli u remoti.

10.1.5 P26S – Politika tas-Sigurtà ta' Partijiet Terzi u tal-Fornituri: Tiżgura li fornituri li jaċċessaw jew jirreġistraw data għall-organizzazzjoni jsegwu prattiki ta' ħin sinkronizzat fuq bażi kuntrattwali.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001:

11.1.1 Klawżola 8.1 – Teħtieġ l-implimentazzjoni tal-kontrolli meħtieġa għal operazzjonijiet siguri, inklużi logging u timestamping.

11.2 ISO/IEC 27002:

11.2.1 Kontroll 8.17 – Jirrakkomanda ħin sinkronizzat għas-sistemi kollha li jipproduċu logs jew joperaw b'mod kollaborattiv.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Jeħtieġ l-użu ta' sorsi tal-ħin interni jew esterni għall-preċiżjoni tat-timestamp tal-logs.

11.3.2 SC-45 – Jispeċifika l-użu ta' sorsi NTP fdati u l-prevenzjoni ta' tibdil manwali tal-ħin f'sistemi kritiċi.

11.4 GDPR tal-UE:

11.4.1 Artikolu 5(1)(d) – Jeħtieġ preċiżjoni u accountability fl-ipproċessar tad-data personali, appoġġjati minn timestamps sinkronizzati.

11.4.2 Artikolu 32 – Jeħtieġ miżuri ta' sigurtà li jiżguraw l-integrità tad-data, inklużi perjodi ta' logging konsistenti.

11.5 Direttiva NIS2 tal-UE:

11.5.1 Artikolu 21(2)(d) – Jeħtieġ kapacitajiet ta' monitoraġġ u skoperta appoġġjati minn logs tas-sistema sinkronizzati.

11.6 DORA tal-UE:

11.6.1 Artikolu 10 – Jeżiġi reżiljenza operattiva, li tirrikjedi logs ta' inċidenti tal-ICT b'traċċabbiltà u timestamp.

11.6.2 Artikolu 15 – Jeħtieġ li l-fornituri tas-servizzi jżommu reġistri tekniċi preċiżi, inklużi traċċi ta' awditjar b'timestamp.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Jenfasizza l-integrità tat-timestamp għas-sejbien u r-rispons għall-avvenimenti.

11.7.2 MEA03.01 – Jeħtieġ monitoraġġ tal-prestazzjoni bbażat fuq l-evidenza, appoġġjat minn data preċiża sinkronizzata mal-ħin.