| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Daħħal hawn l-isem tal-entità ġuridika rreġistrata | | | | | | | |
| Numru tad-dokument:<br>P23 | | | | | Titlu tad-dokument:<br>**Politika dwar is-Sinkronizzazzjoni tal-Ħin** | | | | | | | |
| Verżjoni:<br>1.0 | | Data tad-dħul fis-seħħ:<br>01.01.2025 | | | Sid tad-dokument: | | | | | | | |
| X | Politika | | Standard | | Proċedura | | Formola | | Reġistru | | Oħra | |

| **Storja tar-reviżjonijiet** | | | | |
|---|---|---|---|---|
| **Numru tar-reviżjoni** | **Data tar-reviżjoni** | **Bidliet** | **Ivrevedut minn** | **Sid tal-proċess** |
| | | | | |
| | | | | |

| **Approvazzjonijiet** | | | |
|---|---|---|---|
| **Isem** | **Pożizzjoni** | **Data** | **Firma** |
| | | | |
| | | | |

Allinjata ma’ standards u regolamenti

| Standard/Regolament | Klawżola/Artikolu | Kumment |
|---|---|---|
| ISO/IEC 27001:2022 | Klawżola 8 | - |
| ISO/IEC 27002:2022 | Kontroll 8 | - |
| NIST SP 800-53 Rev.5 | SC-45, AU-8 | - |
| GDPR tal-UE | Artikolu 32 | - |
| Direttiva NIS2 tal-UE | Artikolu 21(2)(e) | - |
| DORA tal-UE | Artikoli 9, 10 | - |
| COBIT 2019 | DSS05.04, MEA | - |

**1. Għan**

1.1 L-għan ta’ din il-politika huwa li jiġi żgurat li s-sistemi, l-applikazzjonijiet, l-apparati u s-servizzi kollha tal-cloud tal-organizzazzjoni jżommu konfigurazzjonijiet tal-ħin konsistenti u preċiżi permezz tas-sinkronizzazzjoni ma’ sorsi tal-ħin magħżula u fdati.

1.2 Is-sinkronizzazzjoni preċiża tal-ħin hija essenzjali għal logging affidabbli, komunikazzjonijiet siguri, traċċabbiltà għall-awditjar, rispons għall-inċidenti u investigazzjoni forensika. Ħin mhux allinjat jista’ jwassal għal logs li ma jkunux jistgħu jiġu korrelati, fallimenti fl-awtentikazzjoni u rappurtar regolatorju mhux komplut.

1.3 Din il-politika tappoġġa l-Kontroll 8.17 tal-Anness A ta’ ISO/IEC 27001 u standards internazzjonali relatati billi timponi preċiżjoni tal-ħin u skoperta tad-devjazzjoni tal-arloġġi fl-assi tal-IT tal-organizzazzjoni.

**2. Kamp ta’ applikazzjoni**

**2.1 Din il-politika tapplika għal:**

2.1.1 Il-komponenti kollha tal-infrastruttura, inklużi servers, workstations, apparati tan-network, firewalls u sistemi tal-IoT

2.1.2 Ambjenti virtwali u tal-cloud (eż. AWS, Azure, Google Cloud)

2.1.3 Is-sistemi kollha li jipparteċipaw fil-logging, fl-awtentikazzjoni, fl-ipproċessar tat-tranżazzjonijiet jew fil-korrelazzjoni tal-avvenimenti ta’ sigurtà

2.1.4 L-impjegati interni, il-kuntratturi u l-forniturі terzi ta’ servizzi kollha li għandhom responsabbiltà għal sistemi sensittivi għall-ħin

2.2 Is-sistemi li jiġġeneraw jew jużaw reġistri bit-timestamps — bħal entrati fil-logs, twissijiet, reġistri tal-attività tal-utenti jew evidenza forensika — huma meqjusa fil-kamp ta’ applikazzjoni.

**3. Objettivi**

3.1 Tiġi definita arkitettura konsistenti u ċentralizzata għas-sinkronizzazzjoni tal-ħin bl-użu ta’ sorsi NTP approvati jew ekwivalenti.

3.2 Jiġi żgurat li s-sistemi kollha jissinkronizzaw l-arloġġi tagħhom f’intervalli definiti u li kull devjazzjoni tiġi skoperta u kkoreġuta awtomatikament jew b’intervent minimu.

**3.3 Tinżamm il-preċiżjoni tal-arloġġi f’ambjenti ibridi, fuq il-post u tal-cloud sabiex ikun possibbli:**

3.3.1 Korrelazzjoni affidabbli tal-avvenimenti u rispons għall-inċidenti

3.3.2 Konformità regolatorja ma’ standards bħal ISO 27001, GDPR, NIS2 u DORA

3.3.3 Protezzjoni kontra replay attacks u fallimenti ta’ awtentikazzjoni bbażati fuq il-ħin

3.4 Jiġu stabbiliti rwoli ċari, proċeduri għall-ġestjoni tal-eċċezzjonijiet u mekkaniżmi ta’ awditjar biex tinżamm l-applikazzjoni ta’ din il-politika.

3.5 Jiġi żgurat li anomaliji relatati mal-ħin jiġu rreġistrati fil-logs, jiġġeneraw twissijiet u jiġu eskalati meta jaqbżu t-tolleranzi stabbiliti.

**4. Rwoli u responsabbiltajiet**

**4.1 Uffiċjal Kap tas-Sigurtà tal-Informazzjoni (CISO)**

4.1.1 Huwa s-sid ta’ din il-politika u jiżgura l-allinjament mal-kontrolli operattivi tal-ISMS u mar-rekwiżiti regolatorji.

4.1.2 Japprova l-għażla tas-sors tal-ħin fil-livell tal-intrapriża u jivverifika l-proċessi ta’ rappurtar dwar is-sinkronizzazzjoni tal-ħin.

**4.2 Maniġer tas-Servizzi tal-Infrastruttura / Responsabbli tal-Inġinerija tan-Network**

4.2.1 Iżomm is-servers NTP primarji u sekondarji tal-organizzazzjoni jew il-konfigurazzjoni tas-sors tal-ħin magħżul.

4.2.2 Jiżgura li l-apparati kollha konnessi man-network u l-istanzi virtwali jissinkronizzaw il-ħin f’intervalli xierqa.

4.2.3 Jimmonitorja l-logs tas-sinkronizzazzjoni tal-ħin, it-twissijiet tad-devjazzjoni tal-arloġġ u l-kundizzjonijiet ta’ ħsara.

[ ... 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 Din il-politika għandha tiġi rieżaminata kull sena, jew qabel jekk iseħħ xi waħda mill-kundizzjonijiet li ġejjin:**

9.1.1 Skoperta ta’ exploits ibbażati fuq il-ħin jew fallimenti fil-logging

9.1.2 Bidliet fl-infrastruttura ewlenija tal-ħin (eż. servers NTP ġodda fil-livell tal-intrapriża jew aġġornamenti tal-protokolli)

9.1.3 Diskrepanzi fid-devjazzjoni tal-ħin fuq pjattaformi tal-cloud jew bidliet fis-servizzi reġjonali

9.1.4 Sejbiet wara l-inċident li jidentifikaw nuqqas ta’ allinjament tal-ħin bħala fattur li kkontribwixxa

9.2 Ir-rieżami għandu jiġi kkoordinat mir-Responsabbli tal-Infrastruttura, b’kontribut obbligatorju mis-SOC, mis-Sigurtà tal-Applikazzjonijiet u mill-partijiet interessati tal-konformità.

9.3 Ir-reviżjonijiet għandhom jiġu dokumentati fir-Reġistru tad-Dokumenti tal-ISMS u kkomunikati lill-partijiet interessati interni u esterni affettwati.

9.4 Verżjonijiet storiċi tal-politika għandhom jiġu arkivjati b’mod sigur, miżmuma taħt kontroll tal-verżjoni u magħmula disponibbli għal talbiet ta’ awditjar ta’ konformità jew ta’ natura legali.

**10. Politiki relatati u rabtiet**

10.1 P1 – Politika tas-Sigurtà tal-Informazzjoni. Tistabbilixxi l-mandat ġenerali biex tiġi żgurata l-integrità u t-traċċabbiltà tas-sistemi kollha tal-informazzjoni, li għalihom il-preċiżjoni tal-ħin hija element fundamentali.

10.2 P5 – Politika tal-Ġestjoni tat-Tibdil. Tirregola modifiki fil-konfigurazzjonijiet tas-sistema, inklużi aġġustamenti tas-sors tal-ħin, u tiżgura dokumentazzjoni, ittestjar u pjanijiet ta’ treġġigħ lura xierqa.

10.3 P22 – Politika tal-Logging u l-Monitoraġġ. Tiddependi direttament fuq ħin sinkronizzat biex tiżgura s-sekwenzjar tal-avvenimenti, il-korrelazzjoni tal-logs u l-integrità tal-investigazzjoni tal-inċidenti f’sistemi differenti.

10.4 P30 – Politika dwar ir-Rispons għall-Inċidenti. Tiddependi fuq timestamps preċiżi għal investigazzjonijiet forensiċi, skedi taż-żmien tal-inċidenti u evidenza tal-chain of custody. Ħin mhux preċiż idgħajjef il-kredibbiltà tar-rapporti tal-inċidenti.

10.5 P20 – Politika tal-Protezzjoni tal-Endpoint / Malware. Teħtieġ twissijiet f'waqthom u analiżi tal-imġiba biex jinstabu t-tixrid tal-malware, il-moviment laterali u anomaliji fl-aċċess.

10.6 P6 – Politika tal-Ġestjoni tar-Riskju. Tiddefinixxi n-nuqqas ta' sinkronizzazzjoni bħala riskju operattiv u forensiku potenzjali, u teħtieġ il-kontrolli definiti f'din il-politika biex jitnaqqas l-impatt.

## 11. Standards u oqfsa ta' referenza

### 11.1 ISO/IEC 27001

11.1.1 Klawżola 8.1 – Ippjanar u Kontroll Operattiv: Teħtieġ l-integrazzjoni ta' kontrolli tekniċi preċiżi, bħal arloġġi tas-sistema sinkronizzati, għal eżekuzzjoni operattiva affidabbli.

### 11.2 ISO/IEC 27002:2022 – Kontroll 8

11.2.1 Isaħħaħ il-preċiżjoni tal-arloġġ u jobbliga konsistenza organizzattiva fil-ħin tas-sistema biex jiffaċilita l-paragun tal-logs, l-investigazzjoni u l-verifika sigura tat-tranżazzjonijiet.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – Sinkronizzazzjoni tal-Ħin tas-Sistema: Teħtieġ sinkronizzazzjoni tal-ħin bl-użu ta' sorsi awtorevoli fil-komponenti kollha fi ħdan il-konfini tas-sistema.

11.3.2 AU-8 – Time Stamps: Tiżgura li l-avvenimenti jingħataw timestamp b'mod preċiż u tipprovdi traċċabbiltà għall-awditjar u għar-rispons għall-inċidenti.

### 11.4 GDPR tal-UE (2016/679)

11.4.1 Artikolu 32 – Sigurtà tal-Ipproċessar: Għalkemm ma jsemmix b'mod espliċitu l-ħin, jobbliga l-użu ta' miżuri tekniċi xierqa — inklużi traċċi tal-awditjar u logs — li intrinsikament jiddependu fuq timestamps sinkronizzati għall-validità u l-integrità tagħhom.

### 11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikolu 21(2)(e): Teħtieġ kapaċitajiet ta' logging u skoperta li jippreżupponu sinkronizzazzjoni preċiża tal-ħin għall-korrelazzjoni bejn sistemi u għal rispons f'waqtu.

### 11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 9 – Ġestjoni tar-Riskju tal-ICT: Jobbliga telemetrija preċiża tas-sistema għall-monitoraġġ tar-riskju u l-iskoperta ta' anomaliji, li tiddependi fuq sinkronizzazzjoni preċiża tal-arloġġi.

11.6.2 Artikolu 10 – Kontinwità tan-Negozju tal-ICT: Jimponi kontrolli li jiżguraw l-integrità tas-sistema waqt tfixkil, inklużi reġistri ta' avvenimenti allinjati fil-ħin.

### 11.7 COBIT 2019

11.7.1 DSS05.04 – Monitor Security Events: Jeħtieġ integrità tat-timestamps għal analiżi effettiva tal-logs u sejbien tat-theddid.

11.7.2 MEA03 – Monitor, Evaluate, and Assess Compliance: Is-sinkronizzazzjoni tal-ħin tappoġġa awditjar ta' konformità preċiż u ċikli ta' rappurtar.