

				Dañhal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P14				Titlu tad-dokument: Politika taż-żamma u r-rimi tad-data							
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	Klawżoli 6.1.3, 8.1	
ISO/IEC 27002:2022	Kontrolli 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
GDPR tal-UE	Artikoli 5(1)(e), 17, 32	
Direttiva NIS2 tal-UE	Artikolu 21(2)(a-e)	
DORA tal-UE	Artikoli 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Għan

1.1 L-għan ta' din il-politika huwa li tiddefinixxi r-rekwiżiti organizzattivi għaż-żamma tad-data u għar-rimi sigur tagħha tul il-fażijiet kollha taċ-ċiklu tal-ħajja tal-informazzjoni. Din tiżgura l-konformità mal-obbligi legali, regolatorji u kuntrattwali applikabbli, u tipprevjeni l-akkumulazzjoni mhux meħtieġa jew riskjuża tad-data.

1.2 Din il-politika tappoġġa l-implimentazzjoni tal-ISO/IEC 27001:2022 billi timponi kontroll fuq il-perjodi ta' ħażna tad-data u fuq prattiki ta' rimi irriversibbli. Din tippermetti dokumentazzjoni traċċabbli tar-reġistri, timponi żamma allinjata mas-sensittività tal-klassifikazzjoni, u tiżgura li l-organizzazzjoni tkun lesta għall-awditjar, għall-ispezzjoni regolatorja u għall-iskoperta legali.

1.3 Barra minn hekk, għandha l-għan li tħares il-Kunfidenzjalità, l-Integrità u d-Disponibbiltà (CIA) tad-data filwaqt li tnaqqas ir-riskju għan-negożju, l-inefficijenzi operattivi u l-esponiment għal ksur tal-privatezza li jirriżultaw minn żamma jew qerda mhux xierqa tad-data.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għall-assi kollha tal-informazzjoni, fiżiċi u diġitali, li huma proprjetà tal-organizzazzjoni, li jiġu pproċessati minnha jew miżmuma minnha, inklużi dawk taħt il-kontroll ta' partijiet terzi, sussidjarji jew sħab ta' esternalizzazzjoni.

2.2 Il-kamp ta' applikazzjoni jinkludi, iżda mhux limitat għal:

- 2.2.1 Dokumenti, fajls u reġistri (diġitali u f'format karta)
- 2.2.2 Bażijiet tad-data u arkivji
- 2.2.3 Imejls u logs tal-messaġġi istantanji
- 2.2.4 Backups, logs tas-sistema u traċċi tal-awditjar
- 2.2.5 Kodiċi sors, data tal-applikazzjoni u assi ospitati fil-cloud
- 2.2.6 Mezzi ta' ħażna rimovibbli u hardwer skadut li fih data

2.3 Il-politika tirregola kemm ir-reġistri operattivi kif ukoll settijiet ta' data rregolata (eż. kontenut finanzjarju, legali, tar-riżorsi umani, relatat mal-klijenti u rilevanti għall-awditjar), irrispettivament mil-lok tal-ħażna jew mis-sistema.

2.4 Din tapplika għad-dipartimenti organizzattivi kollha u għall-impjegati individwali, kuntratturi u fornituri involuti fil-ħolqien, il-ħażna, il-ġestjoni jew ir-rimi tad-data.

3. Obiettivi

3.1 Jiġi żgurati li d-data tinżamm biss sakemm ikun meħtieġ legalment, kuntrattwalment jew operattivament, u li tintrema b'mod sigur meta ma tibqax meħtieġa.

3.2 Jiġi evitat it-tħassir bikri, mhux awtorizzat jew aċċidentali ta' registri meħtieġa għal operazzjonijiet li għadhom għaddejnin, għall-konformità, għal litigazzjoni jew għal skopijiet ta' awditjar.

3.3 Jiġu stabbiliti u applikati skedi ta' żamma konsistenti bbażati fuq il-klassifikazzjoni tal-informazzjoni, it-tip ta' assi, il-liġijiet applikabbli u l-esponiment għar-riskju.

3.4 Tifhars il-privatezza u l-kunfidenzjalità tad-data matul il-perjodu taż-żamma tagħha u fil-mument tar-rimi tagħha, inkluż it-tweġiq tad-drittijiet tas-suġġett tad-data (eż. tħassir skont l-Artikolu 17 tal-GDPR).

3.5 Jiġi żgurati li l-metodi kollha ta' rimi tad-data jkunu irriversibbli, dokumentati kif xieraq u konformi ma' standards rikonoxxuti bħal NIST SP 800-88.

3.6 Jiġi naqqsu l-inefficijenzi operattivi, l-ispejjeż addizzjonali u l-esponiment legali kkwazati minn żamma eċċessiva jew minn data legata mhux traċċata.

3.7 Jiġu appoġġati l-oġettivi ta' kontinwità tan-negozju u ta' rkupru minn diżastru permezz ta' governanza integrata taż-żamma tal-backups u prattiki difensibbli ta' arkivjar tad-data.

4. Rwoġi u responsabbiltajiet

4.1 Maniġment Eżekuttiv

4.1.1 Japprova din il-politika u jiżgura finanzjament, riżorsi u integrazzjoni xierqa fil-programmi ta' ġestjoni tar-riskju tal-intrapriża u tal-konformità.

4.1.2 Iġorr ir-responsabbiltà ġenerali għall-konformità legali u regolatorja relatata maż-żamma tad-data u mar-rimi sigur.

4.2 Uffiċjal Kap tas-Sigurtà tal-Infurmazzjoni (CISO)

4.2.1 Huwa s-sid ta' din il-politika u responsabbli għad-definizzjoni u r-rieżami tal-governanza taż-żamma u tar-rimi f'allinjament mal-ISMS.

4.2.2 Jiżgura li r-reqwiżiti taż-żamma u tar-rimi bbażati fuq il-klassifikazzjoni jiġu implimentati fl-unitajiet tan-negozju u fis-sistemi tekniċi.

4.2.3 Jimmonitorja l-konformità mal-politika u jiżgura azzjoni korrettiva fejn meħtieġ.

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

9. Reqwiżiti għar-rieżami u l-aġġornament

9.1 Din il-politika għandha tiġi rieżaminata kull sena jew meta tintlaħaq kwalunkwe waħda mill-kundizzjonijiet li ġejjin:

9.1.1 Bidliet fil-liġijiet jew regolamenti applikabbli li jaffettwaw iż-żamma tad-data (eż. aġġornamenti għall-GDPR, kodiċijiet tat-taxxa, DORA)

9.1.2 Revizjonijiet tal-qafas tal-klassifikazzjoni jew tal-proċessi tan-negozju li jhallu impatt fuq l-istadji taċ-ċiklu tal-ħajja tad-data

9.1.3 Introduzzjoni ta' sistemi ġodda tal-IT, pjattaformi ta' arkivjar jew teknoloġiji għar-rimi tal-midja

9.1.4 Sejbiet tal-awditjar intern jew rakkomandazzjonijiet regolatorji li jindikaw lakuni fil-prattiki taż-żamma jew tar-rimi

9.2 Ir-rieżami għandu jkun immexxi mis-CISO u mill-Uffiċjal tal-Protezzjoni tad-Data (DPO), b'input minn Legali, Konformità, IT u unitajiet tan-negozju.

9.3 L-Iskeda Ewlenija taż-Żamma tad-Data (MDRS) u r-Registru tar-Rimi għandhom jiġu rieżaminati b'mod parallel biex jiġi żgurati li:

9.3.1 L-iskedi jibqgħu korretti u jirriflettu l-ħtiġijiet operattivi, legali u regolatorji

9.3.2 Id-dokumentazzjoni tar-rimi tkun kompleta u adattata għall-awditjar

9.3.3 Ir-reġistri tal-legal hold jiġu vverifikati u rilaxxati meta xieraq

9.4 Kwalunkwe aġġornament għall-politika għandu:

9.4.1 Jiġi vversonat formalment u miżmum fir-Repożitorju tad-Dokumenti tal-ISMS

9.4.2 Jinkludi storja tar-reviżjonijiet u ġustifikazzjoni għat-tibdil

9.4.3 Jiġi approvat mill-Maniġment Eżekuttiv

9.4.4 Jiġi kkomunikat lill-persunal rilevanti b'taħriġ jew materjal ta' gwida aġġornat

9.5 Fejn iseħhu bidliet sinifikanti fil-politika, l-impjegati affettwati għandhom itemmu taħriġ mill-ġdid immirat fi żmien 30 jum mir-rilaxx biex tiġi żgurata konformità kontinwa.

9.6 Politiki relatati u rabtiet

10. Politiki relatati u rabtiet

10.1.1 P4 - Politika dwar il-Kontroll tal-Aċċess: Tiżgura li individwi awtorizzati biss jaċċessaw id-data matul il-perjodu taż-żamma tagħha u li d-data skaduta tkun ristretta sakemm tintrema.

10.1.2 P12 - Politika tal-Ġestjoni tal-Assi: Tidentifika liema assi jgħorru data li teħtieġ rimi skedat u ssegwi ċ-ċiklu tal-ħajja tagħhom mill-akkwist sal-qerda.

10.1.3 P13 - Politika ta' Klassifikazzjoni u Tikkettar tad-Data: Tiggwida deċiżjonijiet ta' klassifikazzjoni li jinfluwenzaw direttament kemm tinżamm id-data u liema metodu ta' rimi huwa meħtieġ.

10.1.4 P15 - Politika dwar il-Backup u r-Restore: Tiddefinixxi l-perjodi taż-żamma u l-proċeduri ta' rimi għal midja tal-backup u assi ta' data replikati.

10.1.5 P18 - Politika tal-Kontrolli Kriptografiċi: Tappoġġa t-tħassir kriptografiku għar-rimi u timponi iċċifrar waqt il-ħażna tad-data sal-qerda.

10.1.6 P30 - Politika dwar ir-Rispons għall-Inċidenti: Tiġi attivata f'każijiet fejn rimi mhux xieraq jirriżulta f'telf potenzjali ta' data, ksur jew nuqqas regolatorju.

10.2 Kull politika marbuta għandha rwol fl-applikazzjoni ta' mudell koerenti ta' governanza tad-data fil-klassifikazzjoni, il-kontroll taċ-ċiklu tal-ħajja, l-aċċess u l-kapaċità li tintwera l-konformità.

11. Standards u oqfsa ta' referenza

11.1 Din il-politika hija allinjata ma' standards u oqfsa regolatorji rikonoxxuti globalment li jiddefinixxu prattiki siguri, konformi u effiċjenti għall-ġestjoni taċ-ċiklu tal-ħajja tad-data.

11.2 ISO/IEC 27001:

11.2.1 Klawżola 6.1.3 - Pjan ta' Trattament tar-Riskju: Tappoġġa l-mitigazzjoni ta' riskji assoċjati ma' żamma eċċessiva, ksur ta' data jew nuqqasijiet fir-rimi.

11.2.2 Klawżola 8.1 - Ippjanar u Kontroll Operattiv: Tistabbilixxi kontrolli taċ-ċiklu tal-ħajja li jirregolaw il-ħażna, l-arkivjar u l-qerda.

11.3 ISO/IEC 27002:2022 - Kontrolli 5.10, 5.12, 5.30, 5: Jipprovdur gwida prattika dwar l-użu aċċettabbli tad-data, il-ġustifikazzjoni taż-żamma, it-tħassir ikkontrollat u ż-żamma ta' reġistri b'mod difensibbli, allinjati mat-tolleranza għar-riskju tal-organizzazzjoni.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Żamma tar-Reġistri tal-Awditjar: Tiżgura ħażna suffiċjenti ta' logs tal-awditjar u evidenza ta' konformità.

11.4.2 MP-6 - Sanitizzazzjoni tal-Midja: Teħtieġ metodi siguri u dokumentati ta' qerda għal midja fiżika u elettronika.

11.4.3 SI-12 - Immaniġġjar tal-Infurmazzjoni: Jimponi trattament xieraq tad-data allinjat mal-kontrolli taż-żamma u tar-rimi.

11.4.4 PL-2 - Pjan tas-Sigurtà u tal-Privatezza tas-Sistema: Jeħtieġ dokumentazzjoni speċifika għas-sistema dwar il-ġestjoni taċ-ċiklu tal-ħajja tad-data u dispożizzjonijiet għal rimi sigur.

11.5 GDPR tal-UE (2016/679):

11.5.1 Artikolu 5(1)(e) - Minimizzazzjoni tad-Data u Limitazzjoni tal-Ħażna: Jeħtieġ li d-data ma tinżammx aktar milli meħtieġ.

11.5.2 Artikolu 17 - Dritt għat-Tħassir ("id-Dritt li Tinsa"): Jeħtieġ tħassir pront u permanenti ta' data personali fuq talba valida.

11.5.3 Artikolu 32 - Sigurtà tal-Ipproċessar: Isaħħaħ il-protezzjoni tad-data matul iż-żamma u jeħtieġ il-qerda sigura ta' reġistri skaduti.

11.6 Direttiva NIS2 tal-UE (2022/2555):

11.6.1 Artikolu 21(2)(a-e): Jeħtieġ li l-entitajiet jadottaw politiki u miżuri tekniċi għall-ġestjoni sigura tad-data, inklużi limitazzjonijiet tal-ħażna u metodi ta' rimi.

11.7 DORA tal-UE (2022/2554):

11.7.1 Artikolu 5 - Governanza u Kontroll: Jimponi ġestjoni strutturata tar-riskju tal-ICT, inkluża l-ġestjoni sigura taċ-ċiklu tal-ħajja tal-informazzjoni.

11.7.2 Artikolu 9 - Qafas tal-Ġestjoni tar-Riskju tal-ICT: Jeħtieġ politiki għaż-żamma tad-data, il-qerda u l-konformità legali/regolatorja tal-operazzjonijiet diġitali.

11.8 COBIT 2019:

11.8.1 DSS01 - Operazzjonijiet Ġestiti: Jappoġġa t-traċċar taż-żamma u l-konsistenza fis-sistemi tad-data kollha.

11.8.2 DSS05 - Servizzi ta' Sigurtà Ġestiti: Jiżgura l-protezzjoni tad-data maħżuna u arkivjata sal-mument tar-rimi sigur.

11.8.3 MEA03 - Monitoraġġ, Evalwazzjoni u Valutazzjoni tal-Konformità: Jippermetti l-awditjar tal-applikazzjoni taż-żamma, il-proċeduri tat-tħassir u t-twettiq tar-rekwiżiti regolatorji.