					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P18S					Titlu tad-dokument: **Politika tal-Kontrolli Kriptografiċi**							
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**	**Ivrevedut 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 intellettwali 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 ipprojbit u jista' jwassal għal azzjoni legali.

Għal-liċenzjar, ikkuntattja: info@clarysec.com

Allinjata mal-istandards u r-regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	
ISO/IEC 27002:2022	Kontrolli 8.24, 8.25	
NIST SP 800-53 Rev.5	SC-12 sa SC-17	
Direttiva NIS2 tal-UE	Artikoli 21(2)(d), 21(2)(e)	
DORA tal-UE	Artikoli 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
GDPR tal-UE	Artikoli 32(1)(a), 34	

1. Għan

1.1 Din il-politika tistabbilixxi rekwiżiti obbligatorji għall-użu tal-iċċifrar u tal-kontrolli kriptografiċi sabiex jiġu protetti l-Kunfidenzjalità, l-Integrità, id-Disponibbiltà (CIA) u l-awtentiċità tad-data tan-negozju u tad-data personali.

1.2 Tiżgura li l-kontrolli kriptografiċi jintużaw b'mod xieraq fis-sistemi, l-apparati u s-servizzi cloud f'ambjent ta' negozju żgħir.

1.3 Din il-politika tappoġġa direttament iċ-ċertifikazzjoni ISO/IEC 27001:2022 u tgħin lill-organizzazzjoni tissodisfa l-obbligi legali tagħha skont il-GDPR tal-UE, id-Direttiva NIS2 tal-UE u d-DORA tal-UE.

1.4 Il-kontrolli kriptografiċi koperti jinkludu l-iċċifrar tad-data, il-ġestjoni taċ-ċertifikati, il-ġestjoni sigura taċ-ċwievet u backups iċċifrati.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 L-impjegati, il-kuntratturi u l-partijiet terzi kollha li jimmaniġġjaw id-data tal-kumpanija

2.1.2 Is-sistemi tan-negozju, l-endpoints u l-pjattaformi cloud kollha użati biex jaħżnu, jittrasmettu jew jipprovdu aċċess għal informazzjoni Kunfidenzjali

2.1.3 Ir-rekords personali, finanzjarji, legali jew sensittivi kollha kklassifikati skont il-Politika tal-Klassifikazzjoni u t-Tikkettar tad-Data tal-organizzazzjoni

2.1.4 Kull kontroll kriptografiku, inklużi metodi ta' iċċifrar, ċwievet, passwords, ċertifikati u moduli tas-sigurtà

2.2 Il-politika tkopri data maħżuna, data fi tranżitu u data waqt l-użu. Tiggverna wkoll l-iċċifrar użat għall-backups, il-posta elettronika, it-trasferimenti esterni tad-data u s-siti web aċċessibbli pubblikament.

3. Objettivi

3.1 Tiżgura li data sensittiva u data regolata tkun protetta b'miżuri kriptografiċi xierqa f'kull ħin

3.2 Tiddeskrivi r-responsabbiltajiet għall-għażla tal-għodod ta' iċċifrar, l-issettjar tal-konfigurazzjoni u l-ġestjoni taċ-ċwievet

3.3 Tipprevjeni aċċess mhux awtorizzat, tbagħbis jew tnixxija ta' data billi tiżgura kontrolli siguri għat-trażmissjoni u l-ħażna

3.4 Tiżgura konformità mar-rekwiżiti legali u regolatorji li jobbligaw l-iċċifrar tad-data personali u tad-data tan-negozju

3.5 Tżomm is-sigurtà operattiva u d-disponibbiltà billi timmaniġġja ċ-ċertifikati u ċ-ċwievet kriptografiċi b'mod effettiv

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Japprova din il-politika u jiżgura li r-rekwiżiti kriptografiċi jiġu applikati

4.1.2 Jirrieżamina l-eċċezzjonijiet, in-notifiki ta' ksur u l-konformità tal-forniturі mal-klawżoli dwar l-iċċifrar

4.1.3 Jivverifika li s-servizzi esternalizzati jew is-servizzi cloud jissodisfaw l-istandards tal-iċċifrar

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

4.2.1 Jimplimenta u jżomm soluzzjonijiet ta' iċċifrar (eż. iċċifrar sħiħ tad-diska, ċertifikati SSL, VPNs)

4.2.2 Jimmaniġġja ċ-ċiklu tal-ħajja taċ-ċwievet kriptografiċi u l-għodod ta' ħażna sigura

4.2.3 Jikkonfigura u jimmonitorja l-iċċifrar għall-protezzjoni tal-backups, tas-siti web u tal-apparati

[... 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 annwali

9.1.1 Din il-politika trid tiġi rieżaminata mill-inqas darba fis-sena mill-Maniġer Ġenerali, f'koordinazzjoni mal-Fornitur ta' Appoġġ tal-IT u l-Koordinatur tal-Privatezza.

9.2 Attivaturi għal rieżami interim

9.2.1 Għandu jsir rieżami wkoll jekk:

9.2.1.1 Jinbidlu l-istandards jew il-protokolli kriptografiċi (eż. meta algoritmu jiġi rtirat)

9.2.1.2 Jiġu introdotti sistemi jew servizzi cloud ġodda

9.2.1.3 Ksur jew inċident jinvolvi ċavetta jew ċertifikat kompromess

9.2.1.4 Aġġornamenti legali jew regolatorji jaffettwaw ir-rekwiżiti tal-iċċifrar

9.3 Kontroll tal-verżjoni u komunikazzjoni

9.3.1 Il-bidliet kollha fil-politika għandhom jiġu dokumentati f'log tal-kontroll tal-verżjoni

9.3.2 Il-persunal għandu jiġi nnotifikat dwar l-aġġornamenti, u l-verżjonijiet preċedenti għandhom jiġu arkivjati

9.3.3 L-aħħar verżjoni approvata għandha tinżamm fir-repożitorju ċentrali tal-politiki

10. Politiki relatati u rabtiet

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

10.1.1 P12S – Politika tal-Ġestjoni tal-Assi: Tiżgura li l-iċċifrar jiġi applikat għall-assi kklassifikati waqt il-ħażna, it-trasferiment u r-rimi.

10.1.2 P14S – Politika taż-Żamma u r-Rimi tad-Data: Tiddeskrivi l-perjodi ta' żamma u tirrikjedi ħażna iċċifrata tad-data sakemm titħassar b'mod sigur.

10.1.3 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tallinja l-iċċifrar mal-prinċipji tal-protezzjoni tad-data u l-aspettattivi regolatorji skont l-Artikolu 32 tal-GDPR.

10.1.4 P22S – Politika tal-Illoggjar u l-Monitoraġġ: Tirrikjedi logging tal-użu taċ-ċwievet, fallimenti tal-iċċifrar u skadenzi taċ-ċertifikati għal finijiet ta' awditjar.

10.1.5 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiddettalja l-mogħdijiet ta' eskalazzjoni, it-trażżin u l-proċeduri ta' notifika meta l-iċċifrar ifalli jew iċ-ċwievet jiġu kompromessi.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 8.1 – Tirrikjedi l-implimentazzjoni ta’ kontrolli operattivi, inkluż l-iċċifrar, biex jiġu ġestiti r-riskji ta’ sigurtà.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.24 – Jiddeskrivi r-rekwiżiti għall-applikazzjoni tal-iċċifrar għall-kunfidenzjalità u l-integrità.

11.2.2 Kontroll 8.25 – Jiddeskrivi l-ġestjoni sigura taċ-ċwievet kriptografiċi u taċ-ċertifikati.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-12 – Jistabbilixxi r-rekwiżiti għall-istabbiliment u l-verifika taċ-ċwievet kriptografiċi.

11.3.2 SC-13 – Jiddefinixxi standards għall-ġenerazzjoni taċ-ċwievet kriptografiċi.

11.3.3 SC-17 – Ikopri l-infrastruttura taċ-ċavetta pubblika (PKI) u l-ġestjoni taċ-ċiklu tal-ħajja taċ-ċertifikati.

11.3.4 SC-28 – Jeħtieġ l-iċċifrar ta’ data maħżuna.

11.3.5 SC-12 sa SC-17 (familja) – Jiżgura li l-protezzjonijiet kriptografiċi jiġu implimentati b’mod xieraq fis-sistemi kollha.

11.4 GDPR tal-UE

11.4.1 Artikolu 32(1)(a) – Jeħtieġ li l-organizzazzjonijiet jimplimentaw miżuri tekniċi bħall-iċċifrar biex jiżguraw il-kunfidenzjalità tad-data.

11.4.2 Artikolu 34 – Jistabbilixxi li l-iċċifrar jista’ jeżenta lill-organizzazzjonijiet minn notifiki ta’ ksur jekk id-data tkun ma tinftiehemx minn persuni mhux awtorizzati.

11.5 Direttiva NIS2 tal-UE

11.5.1 Artikolu 21(2)(d) – Jeħtieġ iċċifrar effettiv biex jiġu protetti s-sistemi u l-komunikazzjonijiet.

11.5.2 Artikolu 21(2)(e) – Jenfasizza l-protezzjoni tad-data u l-mitigazzjoni tat-theddid ċibernetiku permezz tal-iċċifrar.

11.6 DORA tal-UE

11.6.1 Artikolu 6(2)(d) – Jeħtieġ li s-sistemi tal-ICT iżommu kanali ta’ komunikazzjoni siguri u iċċifrar.

11.6.2 Artikolu 9(2)(f) – Jobbliga lill-entitajiet finanzjarji jużaw iċċifrar b’saħħtu biex jipproteġu l-komunikazzjonijiet diġitali u l-iskambji tad-data.

11.7 COBIT 2019

11.7.1 DSS05.01 – Jobbliga l-protezzjoni ta’ informazzjoni sensittiva permezz tal-iċċifrar u protokolli kriptografiċi.

11.7.2 APO13.02 – Jeħtieġ implimentazzjoni effettiva ta’ kontrolli tas-sigurtà, inklużi salvagwardji kriptografiċi, bħala parti mill-ippjanar tas-sigurtà tal-informazzjoni.