					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P29S					Titlu tad-dokument: **Politika dwar id-Data tat-Test u l-Ambjent tat-Test**						
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 ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżoli 6.1, 8	
ISO/IEC 27002:2022	Kontrolli 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
GDPR tal-UE	Artikoli 5(1)(c), 25, 32	
Direttiva NIS2 tal-UE	Artikolu 21(2)(e), (h)	
DORA tal-UE	Artikolu 9	
COBIT 2019	BAI07, DSS05	

1. Għan

1.1 Din il-politika tiddefinixxi kif id-data tat-test u l-ambjenti tat-test għandhom jiġu ġestiti biex jiġi evitat esponiment aċċidentali, ksur tad-data jew tfixkil operattiv waqt attivitajiet ta’ ttestjar.

1.2 Tiżgura li data reali tal-klijenti qatt ma tintuża b’mod mhux xieraq waqt l-ittestjar tas-softwer jew tas-sistemi u li l-ambjenti tat-test ikunu separati b’mod loġiku u tekniku mis-sistemi tal-produzzjoni.

1.3 Din il-politika hija mfassla biex tgħin lill-SMEs jikkonformaw mar-rekwiżiti taċ-ċertifikazzjoni ISO/IEC 27001 u mal-liġijiet rilevanti dwar il-protezzjoni tad-data, filwaqt li tibqa’ prattika u applikabbli għal organizzazzjonijiet mingħajr tim tal-IT dedikat.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 L-ambjenti tat-test kollha (eż. ambjenti ta’ staging, sistemi sandbox, testbeds tal-iżvilupp)

2.1.2 Id-data tat-test kollha, kemm jekk maħluqa manwalment, iġġenerata jew derivata minn sistemi live

2.1.3 Il-persunal kollu involut fl-attivitajiet ta’ ttestjar, inklużi impjegati, kuntratturi, freelancers u fornituri ta’ servizzi tal-IT

2.1.4 Kull ttestjar li jista’ jkollu impatt fuq pjattaformi aċċessibbli għall-klijenti, sistemi interni tan-negozju jew servizzi ta’ partijiet terzi

2.2 Tkopri kemm l-ambjenti tekniċi kif ukoll il-proċessi użati biex jappoġġjaw:

2.2.1 L-iżvilupp ta’ websajts, applikazzjonijiet u għodod

2.2.2 Titjib fis-sistemi, ittestjar tal-konfigurazzjoni u tal-integrazzjoni

2.2.3 Testijiet funzjonali jew tas-sigurtà, kemm awtomatizzati kif ukoll manwali

3. Objettivi

3.1 Jiġi evitat l-użu ta’ data reali u identifikabbli tal-klijenti fl-ittestjar sakemm ma tkunx anonimizzata u approvata b’mod espliċitu.

3.2 Tinżamm separazzjoni stretta bejn is-sistemi tat-test u dawk tal-produzzjoni biex jiġi evitat esponiment mhux intenzjonat tad-data jew interferenza operattiva.

3.3 Jiġu protetti s-sistemi u d-data tat-test kontra aċċess mhux awtorizzat, żvelar aċċidentali jew użu mill-ġdid bejn ambjenti differenti mingħajr kontrolli xierqa.

3.4 Tiġi żgurata l-konformità mar-regolamenti rilevanti dwar il-protezzjoni tad-data (eż. GDPR, NIS2) billi d-data tat-test kollha tiġi proċessata b'mod legali, ġust u sigur.

3.5 Tiġi appoġġjata l-kapaċità tal-organizzazzjoni li turi konformità f'awditi esterni u għaċ-ċertifikazzjoni ISO/IEC 27001 billi jiġu dokumentati l-prattiki ta' ttestjar u jiġu applikati salvagwardji konsistenti.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Għandu r-responsabbiltà ġenerali għall-protezzjoni tad-data tat-test u għas-sigurtà tas-sistemi tat-test.

4.1.2 Japprova kull użu ta' data reali fl-ittestjar wara li jikkonferma li hemm salvagwardji xierqa fis-seħħ (eż. anonimizzazzjoni jew masking tad-data).

4.1.3 Jivverifika li l-attivitajiet ta' ttestjar ikunu dokumentati kif xieraq u konformi ma' din il-politika.

4.2 Sid tal-Proġett

4.2.1 Jikkoordina t-tfassil u l-eżekuzzjoni tal-proċessi ta' ttestjar.

4.2.2 Jiżgura li l-membri kollha tat-tim jifhmu u jsegwu din il-politika.

4.2.3 Jikkonferma li s-sistemi tat-test huma kkonfigurati b'mod sigur qabel ma jibda l-ittestjar.

4.2.4 Jirrapporta lill-GM kull inċident li jinvolvi ambjenti tat-test jew tnixxijiet ta' data.

[... 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 Rieżamijiet skedati

9.1.1 Din il-politika għandha tiġi rieżaminata mill-inqas darba fis-sena mill-Maniġer Ġenerali (GM). Ir-rieżami għandu jiżgura li l-politika tibqa' aġġornata ma':

9.1.1.1 Bidliet fl-għodod, fil-pjattaformi jew fl-ambjenti tal-iżvilupp tas-softwer

9.1.1.2 Obbligi legali aġġornati, inklużi rekwiżiti dwar il-protezzjoni tad-data jew ir-reżiljenza diġitali

9.1.1.3 Iċ-ċertifikazzjoni tal-SME u l-kapaċità li tintwera l-konformità taħt ISO/IEC 27001

9.2 Avvenimenti li jattivaw rieżami interim

9.2.1 Għandhom isiru rieżamijiet addizzjonali wara:

9.2.1.1 Kull inċident li jinvolvi esponiment ta' data jew kompromess f'ambjenti tat-test

9.2.1.2 Użu ta' data reali fl-ittestjar, anke jekk anonimizzata

9.2.1.3 Introduzzjoni ta' metodi, sistemi jew forniturigodda għat-test

9.2.1.4 Aġġornamenti regolatorji li jaffettwaw kif tiġi ġestita d-data waqt l-ittestjar

9.3 Ġestjoni tat-tibdil u komunikazzjoni

9.3.1 Il-GM huwa responsabbli għal:

9.3.1.1 L-aġġornament ta' din il-politika u d-dokumentazzjoni ta' kull reviżjoni bi storja tal-verżjonijiet

9.3.1.2 In-notifika lill-persunal, lill-iżviluppaturi u lill-fornituri tas-servizzi rilevanti dwar l-aġġornamenti

9.3.1.3 Il-konferma li l-persunal kollu involut fl-ittestjar jifhem u japplika l-aħħar regoli

9.3.1.4 Iż-żamma ta' verżjoni aċċessibbli tal-aħħar politika għar-rieżami u għall-awditjar

9.4 Awditjar u dokumentazzjoni

9.4.1 Ir-reġistri tar-rieżamijiet kollha tal-politika, l-approvazzjonijiet għall-użu ta' data reali u kull ġustifikazzjoni ta' eċċezzjoni għandhom:

9.4.1.1 Jinżammu b'mod sigur għall-finijiet tal-awditjar

9.4.1.2 Ikunu disponibbli fuq talba waqt awditi interni jew ta' partijiet terzi

9.4.1.3 Jiġu rieżaminati kull sena biex tiġi żgurata l-konsistenza mal-prattiki tat-test

10. Politiki relatati u rabtiet

10.1 Din il-politika għandha tiġi applikata flimkien mal-politiki SME li ġejjin biex jinżammu s-sigurtà u l-konformità waqt l-ittestjar:

10.1.1 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tiddefinixxi min hu responsabbli għas-sorveljanza tal-iżvilupp, l-ittestjar u r-responsabbiltajiet relatati mas-separazzjoni tas-sistemi.

10.1.2 P4S – Politika dwar il-Kontroll tal-Aċċess: Tistabbilixxi l-assenjazzjoni, il-ġestjoni u t-tneħħija tal-kredenzjali tal-aċċess għas-sistemi tat-test.

10.1.3 P8S – Politika dwar l-Għarfien tas-Sigurtà tal-Informazzjoni u t-Taħriġ: Tiżgura li l-persunal jifhem ir-riskji tad-data tat-test, il-prattiki ta' ġestjoni sigura u s-separazzjoni korretta tal-ambjenti.

10.1.4 P13S – Politika ta' Klassifikazzjoni u Tikkettar tad-Data: Tappoġġja klassifikazzjoni ċara tad-data tat-test u tiggwida l-istrateġiji ta' anonimizzazzjoni jew masking.

10.1.5 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tallinja mal-obbligi tal-GDPR, inklużi s-salvagwardji relatati mal-ipproċessar u l-ħażna ta' data personali, anke f'ambjenti mhux ta' produzzjoni.

10.1.6 P24S – Politika dwar l-Iżvilupp Sigur: Tipprovdi l-aspettattivi ġenerali tas-sigurtà għat-timijiet tal-iżvilupp, inkluż l-użu sigur tad-data waqt il-fażijiet tat-test.

10.1.7 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiddeskrivi kif għandu jsir ir-rispons għal kull ksur jew kwistjoni skoperta f'ambjent tat-test jew ikkawżata minn ġestjoni mhux xierqa tad-data tat-test.

10.2 Dawn il-politiki jiffurmaw qafas unifikat tas-sigurtà biex jappoġġjaw l-integrità tat-test, il-minimizzazzjoni tad-data u allinjament sħiħ ma' ISO/IEC 27001 fl-operazzjonijiet tal-iżvilupp u tal-assigurazzjoni tal-kwalità (QA).

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 6.1 – Teħtieġ valutazzjoni tar-riskju u azzjonijiet ta' trattament tar-riskju, inklużi riskji relatati mal-ittestjar.

11.1.2 Klawżola 8.1 – Teħtieġ ippjanar u kontroll tal-proċessi operattivi, inklużi l-arranġamenti għall-ambjenti tas-sistemi tat-test.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.28 – Jeħtieġ li l-organizzazzjonijiet jipproteġu d-data tat-test u jiżguraw li din ma tinkludix data sensittiva jew data live tal-produzzjoni.

11.2.2 Kontroll 8.29 – Jeħtieġ separazzjoni ċara bejn l-ambjenti tal-iżvilupp, tat-test u tal-produzzjoni.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Ikopri l-aspettattivi ta' kontroll għall-iżvilupp u l-ittestjar.

11.3.2 SA-12 – Jindirizza r-riskji tat-test fil-katina tal-provvista u l-valutazzjonijiet tas-sigurtà.

11.3.3 SC-32 – Jeħtieġ separazzjoni tal-ambjenti u protezzjoni tal-kunfidenzjalità u l-integrità tad-data tat-test.

11.4 Regolament Ġenerali dwar il-Protezzjoni tad-Data tal-UE (GDPR)

11.4.1 Artikolu 5(1)(c) – Jeħtieġ minimizzazzjoni tad-data, inkluż l-użu biss tad-data meħtieġa għall-ittestjar.

11.4.2 Artikolu 25 – Jeħtieġ privatezza mid-disinn, li tinkludi wkoll kontrolli tal-ambjent tat-test.

11.4.3 Artikolu 32 – Jobbliga pproċessar sigur ta’ data personali fis-sistemi kollha, inklużi ambjenti mhux ta’ produzzjoni.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikolu 21(2)(e, h) – Jeħtieġ żvilupp sigur u ttestjar tas-sistema, b’mod partikolari fejn servizzi diġitali huma esposti għar-riskju ċibernetiku.

11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 9 – Jenfasizza l-importanza tar-reżiljenza operattiva diġitali, inkluż ittestjar sigur ta’ sistemi tal-ICT minn SMEs fis-settur finanzjarju.

11.7 COBIT 2019

11.7.1 BAI07 – Manage Change Acceptance and Transitioning: Jinkludi kontrolli tat-test biex jiġu vverifikati sistemi ġodda u l-ġestjoni tad-data.

11.7.2 DSS05 – Manage Security Services: Jeħtieġ prattiki ta’ test u żvilupp li jipprevjenu użu ħażin jew esponiment ta’ data tan-negozju.