					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P29					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**

Allinjata mal-istandards u r-regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	Rilevanti għall-ippjanar u l-kontroll operattiv sigur tad-data tat-test u tal-ambjenti tat-test
ISO/IEC 27002:2022	Kontrolli 8.28–8.29	Tkopri d-data tat-test sigura u l-protezzjoni tal-ambjenti tat-test
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Jindirizza l-ittestjar u l-evalwazzjoni mill-iżviluppaturi, il-protezzjoni ta' data maħżuna u l-integrità
GDPR tal-UE	Artikoli 5, 25, 32	Tkopri l-minimizzazzjoni tad-data, il-privatezza mid-disinn u s-sigurtà tal-ipproċessar f'kuntesti ta' ttestjar
Direttiva NIS2 tal-UE	Artikolu 21(2)(e), (h)	Tirrigwarda prattiki siguri ta' żvilupp u ttestjar
DORA tal-UE	Artikolu 9	Tirrigwarda s-sistemi u l-protokolli tal-ICT u s-sigurtà tad-data tat-test
COBIT 2019	DSS05, BAI07	Jindirizza l-ġestjoni tas-servizzi tas-sigurtà u l-aċċettazzjoni u t-tranżizzjoni tat-tibdil

1. Għan

1.1. Din il-politika tistabbilixxi r-rekwiżiti obbligatorji għall-ġestjoni tal-ambjenti tat-test u tad-data tat-test sabiex jiġu żgurati s-sigurtà, il-kunfidenzjalità u l-integrità operattiva tul iċ-ċiklu tal-ħajja tal-iżvilupp u l-ittestjar tas-software.

1.2. Hija għandha l-għan li tipprevjeni aċċess mhux awtorizzat, tnixxija ta' data u kontaminazzjoni tas-sistemi tal-produzzjoni minħabba ambjenti tat-test immaniġġjati ħażin jew l-użu ta' data reali għall-ittestjar.

1.3. Il-politika tirrikjedi ġestjoni sigura tad-data użata għall-ittestjar, hardening tal-infrastruttura tat-test u kontroll tal-aċċess ibbażat fuq ir-rwoli (RBAC), filwaqt li tibqa' allinjata mal-obbligi regolatorji u kuntrattwali applikabbli.

2. Kamp ta' applikazzjoni

2.1. Din il-politika tapplika għall-ambjenti tat-test, għad-data, għall-għodod u għall-proċessi kollha użati għall-ittestjar tas-software, tas-sistemi, tal-applikazzjonijiet u tal-infrastruttura madwar l-organizzazzjoni.

2.2. Hija tkopri:

2.2.1. Ambjenti tat-test ipprovduti fuq il-post, fil-cloud jew permezz ta' pjattaformi ta' partijiet terzi

2.2.2. Data tat-test użata fl-ittestjar funzjonali, tal-prestazzjoni, tar-rigressjoni u tas-sigurtà

2.2.3. Ittestjar manwali, permezz ta' skripts jew awtomatizzat (eż. pipelines ta' CI/CD)

2.2.4. Il-persunal kollu involut fl-ittestjar, inklużi timijiet interni, fornituri u kuntratturi

2.3. Il-politika tapplika irrispettivament mill-kritiċità tas-sistema, mit-tip ta' applikazzjoni jew jekk l-iżvilupp huwiex intern jew esternalizzat.

3. Objettivi

3.1. Li tipprevjeni l-użu ta' data live, sensittiva jew regolata (eż. informazzjoni personali identifikabbli (PII), data tad-detentur tal-karta) f'ambjenti tat-test, sakemm ma tkunx anonimizzata jew approvata b'mod speċifiku.

3.2. Li tiżgura segmentazzjoni tan-network u separazzjoni sħiħa tal-aċċess bejn ambjenti tat-test u tal-produzzjoni sabiex jiġi evitat aċċess mhux awtorizzat għad-data jew kontaminazzjoni tas-sistema.

3.3. Li tirrikjedi iċċifrar, masking jew ġenerazzjoni ta' data sintetika meta tkun meħtieġa data rappreżentattiva għal skopijiet ta' ttestjar.

3.4. Li tnaqqas il-probabbiltà ta' nuqqasijiet ta' konformità, espożizzjoni ta' data tal-klijenti jew tfixkil operattiv li jirriżultaw minn data jew ambjenti tat-test mhux siguri.

3.5. Li tallinja l-ġestjoni tad-data tat-test mal-istandards tal-industrija (ISO, NIST, COBIT) u mar-regolamenti bħall-GDPR, in-NIS2 u d-DORA.

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 salvagwardji tekniċi u amministrattivi għad-data tat-test u għall-ambjenti tat-test.

4.1.2. Japprova l-użu ta' data reali jew sensittiva fl-ittestjar meta jkun hemm ġustifikazzjoni xierqa u kontrolli kumpensatorji.

4.2. Responsabbli tal-QA/Test

4.2.1. Jikkoordinaw l-ippjanar tat-test u jiżguraw li l-attivitajiet kollha tal-ittestjar jikkonformaw mar-rekwiżiti ta' din il-politika.

4.2.2. Jivverifikaw is-separazzjoni xierqa, l-aċċess u t-tħejjija tad-data għal kull faża tal-ittestjar.

[... 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 u aġġornata kif meħtieġ biex tirrifletti:

9.1.1. Bidliet fir-rekwiżiti regolatorji (eż. GDPR, DORA, NIS2)

9.1.2. L-adozzjoni ta' għodod, pjattaformi jew pipelines ta' awtomazzjoni ġodda għall-ittestjar

9.1.3. Sejbiet tal-awditjar intern jew rakkomandazzjonijiet wara inċident

9.1.4. Espansjoni tal-proċessi tal-iżvilupp jew tal-QA li tbiddel il-ġestjoni tad-data tat-test jew l-użu tal-ambjenti

9.2. Is-CISO huwa responsabbli biex jibda r-rieżami f'kollaborazzjoni ma':

9.2.1. Responsabbli tal-QA/Test

9.2.2. Maniġers tad-DevOps u tal-Infrastruttura

9.2.3. Timijiet tal-Iżvilupp tal-Applikazzjonijiet

9.2.4. Data Protection Officer (DPO) u l-konsulent legali

9.3. Ir-rieżamijiet kollha għandhom ikunu:

9.3.1. Taħt kontroll tal-verżjoni u maħżuna fir-repożitorju ċentrali tad-dokumenti

9.3.2. Ikkomunikati lill-persunal affettwat permezz ta' kanali formali (eż. notifiki tal-ISMS, briefings lit-timijiet)

9.3.3. Marbuta ma' aġġornamenti fl-istandards tekniċi, fil-kontrolli u fil-proċeduri operattivi assoċjati

9.4. Rieżamijiet interim ibbażati fuq attivaturi għandhom isiru immedjatament wara kwalunkwe:

9.4.1. Tnixxija ta' data jew ksur li jinvolvi ambjenti tat-test

9.4.2. Nuqqas ta' konformità tal-awditjar relatat mal-ġestjoni tad-data tat-test

9.4.3. Bidliet sinifikanti fl-obbligi legali jew fl-arkitettura tal-IT

10. Politiki relatati u rabtiet

10.1. Din il-politika hija integrata mill-qrib mal-politiki li ġejjin biex tiżgura ġestjoni sigura u konformi tad-data tat-test u tal-ambjenti tat-test:

10.1.1. P1 – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi l-prinċipji ġenerali tas-sigurtà li jirregolaw il-protezzjoni tad-data tat-test u l-ġestjoni tal-ambjenti.

10.1.2. P5 – Politika tal-Ġestjoni tat-Tibdil: Tapplika għall-ħolqien, l-aġġornament u d-dekummissjonar tal-ambjenti tat-test u tal-pipelines tal-implimentazzjoni.

10.1.3. P13 – Politika ta' Klassifikazzjoni u Tikkettar tad-Data: Tagħti gwida għall-għażla tad-data tat-test u għall-applikazzjoni ta' kontrolli skont is-sensittività.

10.1.4. P14 – Politika taż-Żamma u r-Rimi tad-Data: Tiddefinixxi l-iskadenzi taż-żamma u r-rekwiżiti ta' rimi sigur għad-datasets tat-test.

10.1.5. P15 – Politika dwar il-Backup u r-Restawr: Tirrikjedi prattiki ta' backup u verifika tal-irkupru għall-ambjenti tat-test.

10.1.6. P18 – Politika tal-Kontrolli Kriptografiċi: Tispeċifika standards obbligatorji tal-iċċifrar għal data maħżuna u data fi tranżitu fi ħdan il-pjattaformi tat-test.

10.1.7. P22 – Politika tal-Illoggjar u l-Monitoraġġ: Tirregola l-viżibbiltà u l-identifikazzjoni ta' anomaliji għall-attivitajiet fl-ambjenti tat-test.

10.1.8. P30 – Politika dwar ir-Rispons għall-Inċidenti: Tiddefinixxi l-eskalazzjoni u r-rimedjazzjoni għal ksur jew inċidenti li jinvolvu sistemi tat-test.

10.1.9. P33 – Politika ta' Monitoraġġ tal-Awditjar u l-Konformità: Tippermetti l-verifika tal-konformità mal-politika u assigurazzjoni kontinwa.

11. Standards u oqfsa ta' referenza

11.1. Din il-politika hija allinjata ma' standards globali taċ-ċibersigurtà u oqfsa regolatorji li jirrikjedu ġestjoni sigura tad-data tat-test u l-protezzjoni ta' ambjenti mhux ta' produzzjoni.

11.2. ISO/IEC 27001:

11.2.1. Klawżola 8.1 - Tirrikjedi ppjanar u kontroll operattiv sigur tad-data tat-test u tal-ambjenti tat-test.

11.3. ISO/IEC 27002:2022 – Kontrolli 8.28–8.29:

11.3.1. Anness A Kontroll 8.28 – Data tat-Test Sigura: Jirrikjedi l-protezzjoni tad-data tat-test użata fil-fażijiet tal-iżvilupp u tal-ittestjar permezz ta' anonimizzazzjoni, masking jew ġenerazzjoni sintetika.

11.3.2. Anness A Kontroll 8.29 – Protezzjoni tal-Ambjenti tat-Test: Jirrikjedi separazzjoni mill-produzzjoni, kontrolli tal-aċċess u hardening tal-ambjent għas-sistemi tat-test.

11.3.3. Dawn il-kontrolli jistabbilixxu rekwiżiti għall-ġestjoni sigura tad-data użata waqt l-ittestjar u għall-protezzjoni ta' sistemi mhux ta' produzzjoni kontra użu ħażin, kompromess jew kontaminazzjoni.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Ittestjar u Evalwazzjoni mill-Iżviluppaturi: Jistabbilixxi aspettattivi għal proċeduri ta' ttestjar siguri u ripetibbli b'kontrolli xierqa tad-data.

11.4.2. SC-28 – Protezzjoni tal-Informazzjoni Maħżuna: Jallinja mal-iċċifrar tad-data tat-test maħżuna f'sistemi mhux ta' produzzjoni.

11.4.3. SC-32 – Integrità tal-Informazzjoni: Jappoġġa l-validazzjoni tad-data, il-prevenzjoni tal-korruzzjoni u kontrolli tal-input/output waqt l-ittestjar.

11.5. GDPR tal-UE (2016/679):

11.5.1. Artikolu 5 – Minimizzazzjoni tad-data: Jipprojbixxi l-użu mhux meħtieġ ta' data personali fl-ittestjar.

11.5.2. Artikolu 25 – Privatezza mid-disinn: Jirrikjedi li tekniki ta' protezzjoni tad-data jiġu applikati mill-bidu taċ-ċiklu tal-iżvilupp u tal-ittestjar.

11.5.3. Artikolu 32 – Sigurtà tal-Ipproċessar: Jobbliga salvagwardji għall-ambjenti tat-test li jimmaniġġjaw data personali jew sensittiva.

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

11.6.1. Artikolu 21(2)(e, h): Jirrikjedi proċessi siguri ta' żvilupp u ttestjar tas-software, b'enfasi fuq il-protezzjoni kontra aċċess mhux awtorizzat u tnixxija ta' data.

11.7. DORA tal-UE (2022/2554):

11.7.1. Artikolu 9 – Sistemi u Protokolli tal-ICT: Jirrikjedi li l-proċessi tal-ittestjar jappoġġaw ir-reżiljenza u jipproteġu d-data operattiva minn kompromess jew żvelar mhux awtorizzat.

11.8. COBIT 2019:

11.8.1. DSS05 – Manage Security Services: Jappoġġa l-applikazzjoni tal-politiki tas-sigurtà fl-ambjenti kollha, inklużi dawk mhux ta' produzzjoni.

11.8.2. BAI07 – Manage Change Acceptance and Transition: Ikopri l-proċess formali tat-tranżizzjoni mill-ittestjar għall-produzzjoni, inklużi kontrolli fuq id-data u fuq l-ambjent.