					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P28S					Titlu tad-dokument: **Politika dwar l-Iżvilupp Esternalizzat**							
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	Klawżoli 5.1, 6.1, 8	Kontrolli tal-ISMS applikabbli u kontrolli relatati mal-forniturі
ISO/IEC 27002:2022	Kontrolli 5.19, 5.20, 8.25–8.27	Kontrolli relatati mal-forniturі u maċ-ċiklu tal-ħajja tal-iżvilupp sigur tas-sistemi
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	Rekwiżiti għall-akkwist, il-katina tal-provvista, l-iżvilupp sigur u l-ftehimiet mal-forniturі
GDPR tal-UE	Artikolu 28	Rekwiżiti kuntrattwali u ta' protezzjoni tad-data għall-ipproċessar minn partijiet terzi
Direttiva NIS2 tal-UE	Artikolu 21(2)(a), (h)	Kontrolli relatati mal-katina tal-provvista u mal-iżvilupp sigur tal-applikazzjonijiet
DORA tal-UE	Artikolu 10	Ġestjoni tar-riskju tal-ICT ta' partijiet terzi, inkluż l-iżvilupp esternalizzat
COBIT 2019	BAI03, DSS05	Rekwiżiti għall-iżvilupp estern u għall-forniturі esterni ta' servizzi tal-IT

1. Għan

1.1 Din il-politika tiżgura li kull żvilupp ta' softwer esternalizzat — kemm jekk jitwettaq minn freelancers, aġenziji jew forniturі terzi — isir b'mod sigur, taħt kontroll kuntrattwali u f'allinjament mar-rekwiżiti legali, regolatorji u ta' awditjar applikabbli.

1.2 Din tipproteġi lill-organizzazzjoni minn riskji relatati ma' kodiċi mhux sigur, sjieda mhux ċara, esponiment tad-data u ġestjoni inadegwata tal-forniturі billi timponi standards ta' żvilupp infurzabbli u sorveljanza tal-forniturі, anke fin-nuqqas ta' dipartiment tal-IT iddedikat.

1.3 Din il-politika tappoġġa ċ-ċertifikazzjoni ISO/IEC 27001:2022 billi tipprovdi aspettattivi ta' żvilupp definiti b'mod ċar, responsabbiltajiet u kontrolli dokumentati fuq attivitajiet ta' żvilupp minn partijiet terzi.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 L-iżviluppaturi esternalizzati kollha, inklużi freelancers u aġenziji tal-iżvilupp

2.1.2 Kull xogħol ta' żvilupp li jinvolvi għodod interni, siti web aċċessibbli pubblikament, applikazzjonijiet tas-softwer jew awtomazzjoni tan-negozju

2.1.3 Persunal responsabbli mill-għażla, il-ġestjoni jew is-sorveljanza ta' żviluppaturi esterni

2.1.4 Kull integrazzjoni ta' sistemi, scripting jew żvilupp minn partijiet terzi li jinteraġixxu ma' data jew sistemi tal-kumpanija

2.2 Tinkludi wkoll kull parti jew pjattaforma b'aċċess għal kredenzjali tal-kumpanija, repożitorji tad-data, repożitorji tal-kodiċi tas-sors, ambjenti ta' staging jew sistemi ta' produzzjoni.

3. Objettivi

3.1 Tiżgura li kull żvilupp esternalizzat jaderixxi ma’ prinċipji ta’ kodifikazzjoni sigura u li l-iżviluppaturi jkunu marbuta kuntrattwalment biex isegwu standards dokumentati u klawżoli ta’ kunfidenzjalità.

3.2 Tistabbilixxi sjieda fuq il-kunsinni kollha — kodiċi, assi, kredenzjali u dokumentazzjoni — filwaqt li tiżgura trasferiment sħiħ tad-drittijiet lill-kumpanija u handover traċċabbli mat-tlestija tal-proġett.

3.3 Tipprevjeni riskji komuni tal-iżvilupp, inkluż l-użu mill-ġdid ta’ kodiċi proprjetarju, attakki fuq il-katina tal-provvista permezz ta’ libreriji, l-użu ta’ frameworks mhux appoġġjati u aċċess amministrattiv mhux ivverifikat.

3.4 Tirrikjedi dokumentazzjoni qabel il-bidu ta’ kull proġett esternalizzat, inklużi kuntratti, Ftehim ta’ Nuqqas ta’ Żvelar u aspettattivi minimi tas-sigurtà.

3.5 Tħares id-data tal-klijenti, is-sistemi u l-proċessi interni billi timponi sorveljanza robusta tal-iżvilupp, ittestjar wara l-kunsinna u ġestjoni sigura tal-aċċess għas-sistemi.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Japprova r-relazzjonijiet kollha mal-forniturі u jiffirma l-ftehimiet tal-iżvilupp.

4.1.2 Jiżgura li kull żvilupp esternalizzat jikkonforma ma’ din il-politika.

4.1.3 Ineħħi l-aċċess għas-sistemi tal-kumpanija wara t-tlestija tal-proġett.

4.1.4 Jirrevedi d-dokumentazzjoni u r-riżultati ta’ wara l-kunsinna.

4.2 Sid tal-Proġett (normalment impjegat intern jew koordinatur maħtur)

4.2.1 Jamministra l-koordinazzjoni ta’ kuljum mal-iżviluppatur estern.

4.2.2 Jivverifika li r-rekwiżiti funzjonali jkunu ntlaħqu u li l-kunsinni jkunu ġew ittestjati.

4.2.3 Jiżgura kunsinna sigura tal-kodiċi u tal-kredenzjali.

4.2.4 Jirrapporta kull kwistjoni jew inċident relatat mal-iżvilupp lill-GM.

[... 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-Maniġer Ġenerali (GM) mill-inqas darba fis-sena. Ir-rieżami jiżgura li din tkompli tissodisfa:

9.1.1.1 ir-rekwiżiti taċ-ċertifikazzjoni ISO/IEC 27001

9.1.1.2 bidliet fl-obbligi legali (eż. Artikolu 28 tal-GDPR, Artikolu 10 tad-DORA)

9.1.1.3 il-prattiki attwali ta’ żvilupp fil-livell tal-SME u r-riskji ta’ partijiet terzi

9.2 Rieżamijiet interim

9.2.1 Ir-rieżamijiet tal-politika għandhom isiru wkoll meta:

9.2.1.1 jiġi integrat fornitur jew pjattaforma ġdida ta’ żvilupp esternalizzat

9.2.1.2 iseħħ inċident sinifikanti li jinvolvi żvilupp esternalizzat

9.2.1.3 ikun hemm bidliet materjali fl-għodod, fil-pjattaformi jew fl-ambjenti użati

9.3 Proċess tar-rieżami

9.3.1 Il-GM huwa responsabbli għal:

9.3.1.1 jivverifika li l-kuntratti, il-Ftehimiet ta’ Nuqqas ta’ Żvelar u l-proċessi tal-kontroll tal-aċċess jibqgħu effettivi

9.3.1.2 jikkonferma li l-forniturі attwali u l-freelancers huma allinjati mal-politika

9.3.1.3 jirrevedi t-termini abbażi tal-feedback minn proġetti jew inċidenti preċedenti

9.4 Kontroll tal-verżjoni u komunikazzjoni

9.4.1 Kull bidla trid tkun:

9.4.1.1 irreġistrata bid-data, ir-raġuni u d-deskrizzjoni tat-tibdil

9.4.1.2 approvata mill-GM u miżjuda mal-istorja tal-verżjonijiet

9.4.1.3 ikkomunikata lill-persunal kollu jew lis-sidien tal-proġetti li jaħdmu ma' żviluppaturi esterni

9.4.1.4 imqassma mill-ġdid lill-fornituri u lill-partijiet terzi affettwati kollha fejn meħtieġ

10. Politiki relatati u rabtiet

10.1 Din il-politika tappoġġa direttament u tiddependi fuq l-implimentazzjoni tal-politiki li ġejjin allinjati mal-SME:

10.1.1 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tiċċara min hu responsabbli għall-approvazzjoni tal-fornituri, il-kontroll tal-aċċess u l-aċċettazzjoni tar-riskju meta jintużaw żviluppaturi esternalizzati.

10.1.2 P4S – Politika dwar il-Kontroll tal-Aċċess: Tiddefinixxi l-ħolqien, ir-restrizzjoni u t-terminazzjoni xierqa tal-kontijiet tal-utenti u tal-aċċess amministrattiv użati waqt żvilupp esternalizzat.

10.1.3 P8S – Politika dwar l-Għarfien tas-Sigurtà tal-Informazzjoni u t-Taħriġ: Tiżgura li l-persunal intern jifhem kif jikkoordina b'mod sigur ma' żviluppaturi esterni, inkluża l-ġestjoni tal-kredenzjali u tal-fajls tal-proġett.

10.1.4 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tistabbilixxi r-rekwiżiti tas-sigurtà u legali għall-ġestjoni ta' data personali li tista' tiġi pproċessata minn żviluppaturi esternalizzati taħt il-GDPR.

10.1.5 P24S – Politika dwar l-Iżvilupp Sigur: Tispeċifika kif l-iżvilupp intern u estern irid isegwi prattiki ta' kodifikazzjoni sigura u verifika ta' libreriji u frameworks.

10.1.6 P30S – Politika dwar ir-Rispons għall-Inċidenti: Meħtieġa meta żvilupp esternalizzat iwassal għal inċidenti tas-sigurtà jew vulnerabbiltajiet, u tiggwida investigazzjoni u rimedjazzjoni koordinati.

10.2 Dawn il-politiki għandhom jiġu implimentati b'mod parallel biex jiġi żgurat li l-iżvilupp esternalizzat ma joħloqx riskju mhux ġestit jew jikser obbligi ta' konformità tal-SME.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 6.1 – L-organizzazzjonijiet għandhom jevalwaw u jittrattaw ir-riskji tas-sigurtà tal-informazzjoni assoċjati mal-fornituri.

11.1.2 Klawżola 8.1 – Tirrikjedi Ippjanar u Kontroll Operattiv, inklużi servizzi minn partijiet terzi bħall-iżvilupp esternalizzat.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.19 – Jirrakkomanda evalwazzjoni tal-kapaċità tal-fornituri biex jissodisfaw ir-rekwiżiti tas-sigurtà tal-informazzjoni.

11.2.2 Kontroll 5.20 – Jinkoraġġixxi monitoraġġ regolari u rieżami perjodiku tas-servizzi minn partijiet terzi.

11.2.3 Kontrolli 8.25–8.27 – Jiddeskrivu prattiki taċ-ċiklu tal-ħajja tal-iżvilupp sigur applikabbli għall-iżvilupp esternalizzat.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – Jeħtieġ li l-istrateġiji tal-akkwist jinkludu miżuri tas-sigurtà tal-informazzjoni.

11.3.2 SA-9 – Jindirizza l-iżvilupp ta' sistemi esterni u r-riskji tal-katina tal-provvista.

11.3.3 SA-11 – Jiddefinixxi prattiki ta' żvilupp sigur, inklużi rieżamijiet tal-kodiċi u r-rimedjazzjoni tad-difetti.

11.3.4 SA-15 – Jinkoraġġixxi għodod awtomatizzati għas-sejbien tad-difetti u l-assigurazzjoni tas-softwer.

11.3.5 SR-3 – Jobbliga li l-ftehimiet mal-forniturijinkludu rekwiżiti taċ-ċibersigurtà.

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

11.4.1 Artikolu 28 – Jeħtieġ kuntratti ma' proċessuri ta' partijiet terzi biex jiżguraw salvagwardji xierqa għall-protezzjoni tad-data, applikabbli direttament għall-iżviluppaturi li jipproċessaw jew jaċċessaw data personali.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikolu 21(2)(a), (h) – Jeħtieġ kontrolli tas-sigurtà tal-katina tal-provvista u prattiki ta' żvilupp sigur tas-softwer għall-forniturita' servizzi diġitali fil-kamp ta' applikazzjoni, inklużi SMEs fejn applikabbli.

11.6 Att dwar ir-Reżiljenza Operattiva Diġitali tal-UE (DORA)

11.6.1 Artikolu 10 – Jeħtieġ ġestjoni tar-riskju tal-ICT ta' partijiet terzi, inklużi ftehimiet tal-iżvilupp, obbligi tas-sigurtà u kontrolli tar-riskju relatati ma' forniturit terzi.

11.7 COBIT 2019

11.7.1 BAI03 – Ġestjoni tal-identifikazzjoni u l-bini tas-soluzzjonijiet – Tiżgura li l-iżvilupp estern jissodisfa r-rekwiżiti tan-negozju u l-aspettattivi tas-sigurtà.

11.7.2 DSS05 – Ġestjoni tas-servizzi tas-sigurtà – Tirrikjedi li s-servizzi esterni tas-sigurtà u l-forniturital-iżvilupp joperaw taħt regoli tas-sigurtà applikati u sorveljanza.