					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P28					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 ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8.1	N/A
ISO/IEC 27002:2022	Kontrolli 5.19-5.22, 8	N/A
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	N/A
GDPR tal-UE	Artikoli 28, 32	N/A
Direttiva NIS2 tal-UE	Artikoli 21(2)(a), (h), 23	N/A
DORA tal-UE	Artikoli 28(1), (2)	N/A
COBIT 2019	APO10, BAI03, DSS	N/A

1. Għan

1.1 Din il-politika tiddefinixxi kontrolli obbligatorji għall-esternalizzazzjoni tal-iżvilupp tas-softwer jew tas-sistemi lil forniturі terzi, kuntratturi jew aġenziji esterni, sabiex tiżgura li prattiki ta’ żvilupp sigur ikunu integrati tul iċ-ċiklu tal-ħajja tal-iżvilupp tas-sistemi.

1.2 Din il-politika għandha l-għan li tipprevjeni vulnerabbiltajiet tas-sigurtà, telf ta’ data, espożizzjoni ta’ proprjetà intellettwali (IP), u nuqqasijiet ta’ konformità li jirriżultaw minn arranġamenti ta’ żvilupp esternalizzat.

1.3 Il-politika tistabbilixxi rekwiżiti għall-governanza tal-fornituri, prattiki ta’ kodifikazzjoni sigura, ġestjoni tal-aċċess, obbligi ta’ monitoraġġ, u proċedura ta’ ħruġ fi tmiem il-kuntratt, sabiex tinżamm il-Kunfidenzjalità, l-Integrità u d-Disponibbiltà (CIA) tas-softwer żviluppat.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għall-unitajiet organizzattivi kollha li jqabbdu entitajiet esterni għall-iżvilupp tas-softwer jew tas-sistemi, inklużi:

2.1.1 applikazzjonijiet tal-web, applikazzjonijiet mobbli, sistemi embedded, interfaces tal-ipprogrammar tal-applikazzjonijiet, scripts, flussi tax-xogħol tal-awtomazzjoni, jew moduli ta’ pjattaforma

2.1.2 żvilupp personalizzat għal pjattaformi interni, sistemi li jiffaċċjaw lill-klijenti, jew prodotti kummerċjali

2.1.3 arranġamenti ma’ żviluppaturi ta’ partijiet terzi, freelancers, aġenziji, jew timijiet offshore

2.2 Il-politika tirregola wkoll kull entità esterna li taċċessa kodiċi sors, ambjenti tat-test, jew pipelines ta’ CI/CD matul l-iżvilupp.

2.3 Ir-rekwiżiti japplikaw irrispettivament mit-tip ta’ kuntratt, il-metodoloġija tal-iżvilupp, jew il-post ġeografiku tal-fornitur esternalizzat.

3. Objettivi

3.1 Jiġi żgurat l-użu ta’ prattiki ta’ żvilupp sigur tul iċ-ċiklu tal-ħajja tal-iżvilupp tas-sistemi (SDLC) fl-arranġamenti kollha esternalizzati, mill-ippjanar sal-verifika ta’ wara l-implimentazzjoni.

3.2 Jiġi żgurat li l-kuntratti kollha ma’ żviluppaturi esterni jinkludu klawżoli obbligatorji dwar il-protezzjoni tad-data, il-kodifikazzjoni sigura, u ż-żamma tal-IP.

3.3 Jiġu ddefiniti rekwiżiti ta’ kontroll tal-aċċess, monitoraġġ, u awditjar għal żviluppaturi ta’ partijiet terzi li jinteraġixxu ma’ sistemi interni.

3.4 Tiġi protetta l-organizzazzjoni minn riskji tal-katina tal-provvista, ksur legali, u dannu reputazzjonali relatat ma’ softwer żviluppat esternament.

3.5 Tinżamm konformità kontinwa ma' oqfsa ta' sigurtà, inkluži ISO/IEC 27001, NIST, GDPR, NIS2, DORA, u COBIT 2019.

4. Rwoli u responsabbiltajiet

4.1 Maniġment Eżekuttiv

4.1.1 Japprova proġetti ta' żvilupp esternalizzat b'riskju għoli u jikkonferma eċċezzjonijiet għall-politika meta dawn ikunu ġġustifikati.

4.1.2 Jiżgura li d-deċiżjonijiet dwar l-esternalizzazzjoni jkunu allinjati mal-objettivi strateġiċi u mal-aptit għar-riskju tal-organizzazzjoni.

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

4.2.1 Japprova l-onboarding tal-fornitur mill-perspettiva tas-sigurtà.

4.2.2 Jiddefinixxi r-rekwiżiti tal-kontrolli tas-sigurtà għal arranġamenti esternalizzati u jirrieżamina rapporti tal-inċidenti.

[... 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 mill-inqas darba fis-sena jew aktar ta' spiss fiċ-ċirkostanzi li ġejjin:

9.1.1 introduzzjoni ta' mudelli ġodda ta' esternalizzazzjoni tal-iżvilupp, fornituri, jew ġurisdizzjonijiet

9.1.2 aġġornamenti għal oqfsa regolatorji bħall-GDPR, NIS2, jew DORA

9.1.3 wara inċident tas-sigurtà tal-informazzjoni li jinvolvi kodiċi, aċċess, jew konsenji esternalizzati

9.1.4 bħala parti minn sejbiet tal-awditjar intern jew titjib fl-ISMS

9.2 L-Uffiċjal Kap tas-Sigurtà tal-Informazzjoni (CISO) huwa responsabbli biex jibda u jikkoordina r-rieżami tal-politika, b'konsultazzjoni ma':

9.2.1.1 Legali u Akkwist (għall-allinjament tal-applikazzjoni kuntrattwali)

9.2.1.2 Sidien tal-Proġett u tal-Prodott (għall-fattibbiltà operattiva)

9.2.1.3 Sigurtà tal-Informazzjoni (għal aġġornamenti dwar it-theddid u l-kontrolli)

9.2.1.4 Maniġment Eżekuttiv (għall-approvazzjoni finali)

9.3 L-aġġornamenti kollha tal-politika għandhom ikunu:

9.3.1.1 taħt kontroll tal-verżjoni u maħżuna f'repożitorju tad-dokumenti maħtur

9.3.1.2 ikkomunikati lill-partijiet interessati involuti f'attivitajiet ta' żvilupp esternalizzat

9.3.1.3 marbuta ma' kwalunkwe aġġornament f'politiki relatati jew dokumentazzjoni proċedurali

9.4 Kull verżjoni tal-politika għandha tkun akkumpanjata minn log tat-tibdil biex tipprovdi traċċabbiltà tal-modifiki u l-approvazzjonijiet.

10. Politiki relatati u rabtiet

10.1 Din il-politika tappoġġja u hija appoġġata mid-dokumenti relatati li ġejjin:

10.1.1 P1 - Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi prinċipji ta' sigurtà fil-livell tal-organizzazzjoni li japplikaw kemm għal kuntesti ta' żvilupp intern kif ukoll għal dawk ta' partijiet terzi.

10.1.2 P5 - Politika tal-Ġestjoni tat-Tibdil: Tiżgura li l-bidliet kollha relatati mal-implimentazzjoni minn bażijiet ta' kodiċi esternalizzati jiġu rieżaminati u approvati qabel l-implimentazzjoni.

10.1.3 P13 - Politika ta' Klassifikazzjoni u Tikkettar tad-Data: Tiddetermina kif data sensittiva tiġi identifikata qabel ma tiġi esposta lil forniturі ta' żvilupp jew lil repożitorji.

10.1.4 P18 - Politika tal-Kontrolli Kriptografiċi: Tagħti gwida dwar kif iċ-ċwievet, is-sigrieti, u l-kredenzjali sensittivi għandhom jiġu mmaniġġjati matul l-iżvilupp u t-twassil.

10.1.5 P24 - Politika dwar l-Iżvilupp Sigur: Tiddefinixxi r-rekwiżiti bażi għall-prattiki ta' żvilupp tas-softwer intern u estern.

10.1.6 P30 - Politika dwar ir-Rispons għall-Inċidenti: Tirregola kif ksur jew kwistjonijiet ta' sigurtà li jinvolvu żvilupp esternalizzat jiġu eskalati, investigati, u riżolti.

10.1.7 P33 - Politika tal-Monitoraġġ tal-Awditjar u l-Konformità: Tipprovdi rekwiżiti għar-rieżami tal-attivitajiet ta' żvilupp esternalizzat waqt awditi jew rieżamijiet tal-konformità.

11. Standards u oqfsa ta' referenza

11.1 Din il-politika hija allinjata ma' oqfsa ta' sigurtà u regolamenti rikonoxxuti internazzjonalment sabiex tiżgura l-esternalizzazzjoni sigura tal-iżvilupp tas-softwer u prattiki robusti ta' ġestjoni tal-forniturі.

11.2 ISO/IEC 27001

11.2.1 Klawżola 8.1 - Ippjanar u Kontroll Operattiv: Tistabbilixxi kontrolli tal-proċess għal żvilupp sigur u twassil minn partijiet terzi.

11.3 ISO/IEC 27002:2022 - Kontrolli 5.19 sa 5.21, 8.

11.3.1 Anness A Kontroll 5.19 - Ġestjoni tar-Relazzjonijiet mal-Fornituri: Jeħtieġ ftehimiet formali bi klawżoli ta' sigurtà u konformità.

11.3.2 Anness A Kontroll 5.20 - L-Indirizzar tas-Sigurtà tal-Informazzjoni fi Ftehimiet mal-Fornituri: Jiżgura li kontrolli speċifiċi għall-iżvilupp ikunu integrati fil-kuntratti.

11.3.3 Anness A Kontroll 5.21 - Ġestjoni tat-Twassil tas-Servizzi tal-Fornitur: Jinvolvi l-monitoraġġ tal-konsenji u r-riskji tal-iżvilupp minn partijiet terzi.

11.3.4 Anness A Kontroll 8.27 - Żvilupp Esternalizzat: Jeħtieġ rekwiżiti ta' sigurtà definiti u kontroll tal-aċċess fuq softwer żviluppat esternament.

11.3.5 Dawn il-kontrolli jiddefinixxu rekwiżiti strutturati għall-għażla, il-kuntrattar, u s-sorveljanza ta' żviluppaturi esternalizzati, inklużi prattiki ta' żvilupp sigur, immaniġġjar tal-kodiċi, u verifika tal-prestazzjoni.

11.4 NIST SP 800-53 Rev.5

11.4.1 SA-4 - Proċess tal-akkwist: Jeħtieġ li r-rekwiżiti ta' żvilupp sigur jiġu definiti fil-ħin tal-akkwist.

11.4.2 SA-9 - Servizzi ta' sistemi esterni: Jirregola kif żviluppaturi ta' partijiet terzi jinteraġixxu b'mod sigur ma' servizzi interni.

11.4.3 SA-10 - Ġestjoni tal-konfigurazzjoni tal-iżviluppatur: Tikkorrispondi ma' obbligi ta' kontroll tal-verżjoni, aċċess għall-kodiċi, u traċċar tat-tibdil għal timijiet esterni.

11.5 GDPR tal-UE (2016/679)

11.5.1 Artikolu 28 - Obbligi tal-proċessur: Jeħtieġ li l-kuntratti ma' żviluppaturi ta' partijiet terzi jispeċifikaw rekwiżiti ta' sigurtà, kontroll, u awditjar għall-immaniġġjar ta' data personali.

11.5.2 Artikolu 32 - Sigurtà tal-ipproċessar: Jeħtieġ salvagwardji xierqa (eż. iċċifrar, kontroll tal-aċċess) meta jiġu żviluppati sistemi li jipproċessaw data personali.

11.6 Direttiva NIS2 tal-UE (2022/2555)

11.6.1 Artikoli 21(2)(a), (h), 23: Jeħtieġu li prattiki ta' żvilupp sigur jiġu applikati fl-arranġamenti kollha ma' partijiet terzi u fil-ktajjen tal-provvista diġitali, b'sorveljanza u verifika teknika.

11.7 DORA tal-UE (2022/2554)

11.7.1 Artikoli 28(1), (2): Jeħtieġu li entitajiet finanzjarji jimmaniġġjaw ir-riskju tal-ICT minn partijiet terzi permezz ta' kontrolli kuntrattwali u sorveljanza ta' żvilupp sigur, b'mod partikolari għal żvilupp esternalizzat kritiku.

11.8 COBIT 2019

11.8.1 APO10 - Ġestjoni tal-Fornituri: Jistabbilixxi rekwiżiti strutturati għall-valutazzjoni tal-fornituri, il-kuntratti, u l-monitoraġġ tal-prestazzjoni.

11.8.2 BAI03 - Ġestjoni tal-Bini tas-Soluzzjonijiet: Tikkorrispondi direttament ma' proċessi siguri ta' SDLC, rieżamijiet tal-kodifikazzjoni, u verifika tal-iżvilupp.

11.8.3 DSS05 - Ġestjoni tas-Servizzi tas-Sigurtà: Tikkorrispondi mal-monitoraġġ u l-protezzjoni ta' sistemi żviluppati esternament jew minn partijiet terzi.