					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P24S					Titlu tad-dokument: **Politika dwar l-Iżvilupp Sigur**							
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	Kontrolli tas-sigurtà rilevanti għall-prattiki operattivi, inkluż l-iżvilupp sigur
ISO/IEC 27002:2022	Kontrolli 8.25–8.27	Tkopri ċ-ċiklu tal-ħajja tal-iżvilupp sigur, l-ittestjar, u r-responsabbiltajiet tas-sigurtà tal-iżviluppaturi ta’ partijiet terzi
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Jindirizza SDLC sigur, kontroll tal-aċċess, u l-ġestjoni tal-vulnerabbiltajiet fl-iżvilupp
GDPR tal-UE	Artikolu 25	Jeħtieġ privatezza mid-disinn u privatezza b’mod awtomatiku fl-iżvilupp tas-softwer
Direttiva NIS2 tal-UE	Artikolu 21(2)(a), (e), (h)	Tobbliga politiki ta’ żvilupp sigur, sorveljanza tal-użu ta’ open-source, u dokumentazzjoni tal-mitigazzjoni
DORA tal-UE	Artikoli 6(7), 9(1)(c), 10(2)(c)	Sigurtà taċ-ċiklu tal-ħajja għal sistemi ICT kritiċi fis-settur finanzjarju
COBIT 2019	BAI	Qafas għall-ġestjoni strutturata tal-iżvilupp sigur, bi traċċabbiltà u reżiljenza

1. Għan

1.1 Din il-politika tiżgura li kull softwer, skripts u għodod ibbażati fuq il-web maħluqa jew modifikati mill-organizzazzjoni jew mis-sħab esterni tagħha jiġu żviluppati b’mod sigur, sabiex jitnaqqas ir-riskju ta’ vulnerabbiltajiet, aċċess mhux awtorizzat għad-data, jew tfixkil operattiv.

1.2 Tistabbilixxi regoli obbligatorji għall-iżvilupp sigur u għall-prattiki ta’ kodifikazzjoni sigura li għandhom jiġu segwiti mill-iżviluppaturi interni kollha, il-kuntratturi u l-fornituri, irrispettivament mid-daqs jew mill-kumplessità tal-proġett.

1.3 Din il-politika hija mfassla biex tipproteġi d-data tal-klijenti, tipprevjeni ksur tad-data, u tiżgura li s-softwer maħluq jew adattat mill-organizzazzjoni jew għaliha jkun jista’ jgħaddi minn awditi tas-sigurtà, jissodisfa r-rekwiżiti legali (eż. GDPR, NIS2, DORA), u jappoġġa ċ-ċertifikazzjoni ISO/IEC 27001.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għall-individwi u l-entitajiet kollha involuti fl-iżvilupp, l-adattament, l-implimentazzjoni, jew il-ġestjoni ta’ dawn li ġejjin f’isem l-organizzazzjoni:

2.1.1 Siti web, applikazzjonijiet, jew għodod ta’ awtomazzjoni

2.1.2 Skripts jew softwer żviluppati internament

2.1.3 Kodiċi maħluq minn żviluppaturi ta’ partijiet terzi jew freelancers

2.1.4 Plugins, libreriji, u komponenti tas-softwer integrati f’sistemi ta’ produzzjoni

2.2 Tkopri l-ambjenti kollha użati f’attivitajiet ta’ żvilupp, inklużi:

2.2.1 Ambjenti ta’ żvilupp u ta’ ttestjar

2.2.2 Ambjenti ta’ staging u ta’ preproduzzjoni

2.2.3 Sistemi ta’ produzzjoni użati biex iħaddmu kodiċi żviluppat apposta

2.3 Il-politika tirregola wkoll il-ġestjoni tad-data waqt l-iżvilupp u l-implimentazzjoni, b’mod partikolari kull użu ta’ data tal-produzzjoni f’ambjent mhux ta’ produzzjoni.

3. Objettivi

3.1 Li jiġi evitat l-introduzzjoni ta’ difetti tas-sigurtà jew vulnerabbiltajiet f’softwer żviluppat apposta jew minn partijiet terzi.

3.2 Li jiġi żgurat li l-prattiki ta’ kodifikazzjoni sigura u l-prevenzjoni tal-vulnerabbiltajiet jiġu integrati f’kull fażi taċ-ċiklu tal-ħajja tal-iżvilupp tas-sistemi.

3.3 Li jitnaqqsu r-riskji assoċjati mal-użu ta’ komponenti open-source jew ta’ partijiet terzi billi tkun obbligatorja l-verifika xierqa u t-traċċar tagħhom.

3.4 Li tkun obbligatorja reviżjoni formali bejn il-pari tal-kodiċi u l-ittestjar tas-sigurtà tal-applikazzjonijiet qabel ir-rilaxx.

3.5 Li jiġi kkontrollat l-aċċess għall-ambjenti ta’ żvilupp u tiġi żgurata s-separazzjoni minn sistemi ta’ produzzjoni live.

3.6 Li jintlaħqu r-rekwiżiti obbligatorji taħt standards u regolamenti internazzjonali (eż. ISO/IEC 27001, GDPR, DORA, NIS2).

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Japprova din il-politika u għandu s-sjieda tagħha.

4.1.2 Jiżgura li kull żvilupp ta’ softwer, kemm intern kif ukoll esternalizzat, ikun konformi ma’ din il-politika.

4.1.3 Jirrevedi u jiffirma kuntratti ta’ żvilupp jew ta’ servizz li jinkludu klawżoli dwar l-iżvilupp sigur.

4.1.4 Jivverifika l-konformità tal-forniturі permezz ta’ kontrolli regolari jew billi jitlob evidenza tas-sigurtà.

4.2 Żviluppatur intern jew sid tal-applikazzjoni

4.2.1 Isegwi prattiki ta’ kodifikazzjoni sigura u proċeduri siguri ta’ implimentazzjoni.

4.2.2 Japplika l-lista ta’ kontroll tal-iżvilupp sigur għal kull proġett.

4.2.3 Jivverifika s-sigurtà ta’ kull komponent open-source jew ta’ parti terza użat.

4.2.4 Jirrapporta kull vulnerabbiltà skoperta lill-GM minnufih.

[... Is-sezzjonijiet 4.3–8 mhumiex inklużi f'dan il-preview. Ixtri d-dokument sħiħ biex taċċessa l-kontenut kollu. ...]

9. Rekwiżiti għar-reviżjoni u l-aġġornament

9.1 Din il-politika għandha tiġi riveduta mill-Maniġer Ġenerali mill-inqas darba fis-sena biex:

9.1.1 Jivverifika l-konformità kontinwa ma’ ISO/IEC 27001, GDPR, NIS2, u DORA

9.1.2 Tirrifletti theddid aġġornat jew bidliet fl-aħjar prattiki tal-iżvilupp sigur

9.1.3 Tiżgura kompatibbiltà ma’ għodod, pjattaformi, jew relazzjonijiet ġodda mal-forniturі

9.2 Reviżjonijiet interim għandhom jiġu skattati minn:

9.2.1 Kwalunkwe inċident tas-sigurtà tal-informazzjoni rrappurtat relatat mas-softwer

9.2.2 L-introduzzjoni ta’ framework ġdid ta’ żvilupp jew pjattaforma ta’ hosting

9.2.3 Bidla fis-sħab tal-iżvilupp ta’ partijiet terzi

9.2.4 Aġġornamenti regolatorji li jaffettwaw l-obbligi tas-softwer jew tas-sigurtà

9.3 Il-bidliet kollha għal din il-politika għandhom ikunu:

9.3.1 Dokumentati bid-data, sommarju tat-tibdil, u approvazzjoni tal-GM

9.3.2 Ikkomunikati b'mod ċar lill-persunal kollu tal-iżvilupp intern u estern

9.3.3 Maħżuna bħala parti mill-kontroll tal-verżjoni u l-istorja tal-verżjonijiet tal-politika tal-organizzazzjoni

9.4 Verżjonijiet aġġornati għandhom ikunu faċli biex jiġu aċċessati, jew permezz ta' pjattaformi interni, dokumentazzjoni stampata, jew servizzi cloud aċċessibbli għall-forniturі.

10. Politiki relatati u rabtiet

10.1 Din il-politika tappoġġa u tiddependi fuq l-implimentazzjoni b'suċċess ta' diversi politiki oħra tal-SME:

10.1.1 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tistabbilixxi responsabbiltà għall-assenjazzjoni u l-verifika tal-kontrolli tas-sigurtà tal-iżvilupp fil-proġetti u fost il-forniturі.

10.1.2 P4S – Politika dwar il-Kontroll tal-Aċċess: Tipprovdi regoli bażiċi biex jiġi limitat l-aċċess għall-ambjenti ta' żvilupp u għar-repożitorji tal-kodiċi, inkluża s-separazzjoni tad-dmirijiet.

10.1.3 P8S – Politika dwar l-Għarfien tas-Sigurtà tal-Informazzjoni u t-Taħriġ: Tiżgura li l-iżviluppaturi interni u l-kuntratturi jifhmu l-prattiki ta' kodifikazzjoni sigura u r-responsabbiltajiet relatati mas-sigurtà.

10.1.4 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tiċċara kif id-data personali għandha tiġi ġestita waqt l-iżvilupp, l-ittestjar, u l-proċessi ta' logging biex tinżamm il-konformità mal-GDPR.

10.1.5 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiddeskrivi kif inċidenti ta' sigurtà relatati mal-iżvilupp għandhom jiġu rrappurtati, evalwati, u rrimedjati, inklużi esponimenti relatati mal-kodiċi.

10.2 Dawn il-politiki jaħdmu flimkien biex jiżguraw li l-iżvilupp sigur ikun jista' jitwettaq u jiġi vverifikat, anke f'organizzazzjoni żgħira jew mhux teknika.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 8.1 – Teħtieġ l-implimentazzjoni ta' kontrolli operattivi, inkluż l-iżvilupp sigur, li jkunu allinjati mal-objettivi tan-negozju u mal-pożizzjoni tar-riskju.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.25 – Jirrakkomanda l-integrazzjoni tas-sigurtà matul iċ-ċiklu tal-ħajja tas-softwer, inkluż kontroll tal-kodiċi sors, kontroll tal-verżjoni, u aċċess tal-iżviluppaturi.

11.2.2 Kontroll 8.26 – Jispeċifika metodi għall-ittestjar tal-applikazzjonijiet u l-verifika tal-funzjonalità tas-sigurtà qabel ma s-sistema tidħol live.

11.2.3 Kontroll 8.27 – Jeħtieġ li l-iżviluppaturi ta' partijiet terzi jżommu mal-istess standards ta' żvilupp u li r-responsabbiltajiet tas-sigurtà tagħhom ikunu definiti b'mod ċar.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 sa SA-15 – Jiddefinixxu proċessi ta' żvilupp sigur, inkluż kontroll tal-aċċess għall-iżviluppaturi, ittestjar, immudellar tat-theddid, u dokumentazzjoni.

11.3.2 SI-10 – Jeħtieġ li l-iżviluppaturi jidentifikaw u jimmitigaw dgħufijiet komuni tas-softwer u li jużaw għodod awtomatizzati fejn applikabbli.

11.4 GDPR tal-UE (2016/679)

11.4.1 Artikolu 25 – “Privatezza mid-disinn u privatezza b’mod awtomatiku” jobbliga l-integrazzjoni ta’ protezzjonijiet tas-sigurtà u tal-privatezza waqt id-disinn u l-iżvilupp tas-softwer, b’mod partikolari fejn tiġi pproċessata data personali.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikolu 21(2)(a), (e), u (h) – Jeħtieġ politiki ta’ żvilupp sigur, sorveljanza tal-użu ta’ open-source, u mitigazzjoni dokumentata tar-riskji relatati mal-applikazzjonijiet f’entitajiet essenzjali u importanti.

11.6 DORA tal-UE (2022/2554)

11.6.1 Artikoli 6(7), 9(1)(c), u 10(2)(c) – Jimponu obbligi ta’ sigurtà fuq iċ-ċiklu tal-ħajja tal-iżvilupp għal entitajiet tas-settur finanzjarju, inklużi SMEs, b’mod partikolari għal sistemi ICT kritiċi.

11.7 COBIT 2019

11.7.1 BAI03 – “Manage Solutions Identification and Build” jappoġġa l-implimentazzjoni ta’ kontrolli ta’ żvilupp strutturati li jenfasizzaw is-sigurtà, it-traċċabbiltà, u r-reżiljenza, adattati għar-restrizzjonijiet tal-SME.