					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P24					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**

1. Għan

1.1 Din il-politika tiddefinixxi rekwiżiti obbligatorji tas-sigurtà għall-attivitajiet ta' żvilupp ta' software u sistemi fi ħdan l-organizzazzjoni, inklużi proġetti interni, żvilupp esternalizzat u integrazzjoni ta' kodiċi minn partijiet terzi.

1.2 L-objettiv huwa li jiġi żgurat li s-sigurtà tkun integrata tul iċ-ċiklu tal-ħajja tal-iżvilupp tas-sistemi u li l-vulnerabbiltajiet jiġu identifikati, mitigati u evitati qabel it-tqegħid fis-servizz fl-ambjent ta' produzzjoni.

1.3 Din il-politika tappoġġa l-applikazzjoni tal-Klawżola 8.1 tal-ISO/IEC 27001:2022 u tal-Kontrolli 8.25–8.28 tal-Anness A billi tistandardizza l-governanza tal-iżvilupp sigur, il-prattiki ta' verifika tal-kodiċi u s-sorveljanza tal-iżvilupp minn partijiet terzi.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għal dawn kollha:

2.1.1 Software, applikazzjonijiet, scripts, integrazzjonijiet u għodod ta' awtomazzjoni żviluppati internament jew esternament

2.1.2 Timijiet tal-iżvilupp, sidien tal-prodott, timijiet DevOps, assigurazzjoni tal-kwalità (QA), periti, maniġers tal-proġett u kuntratturi

2.1.3 Ambjenti tal-iżvilupp tul iċ-ċiklu tal-ħajja tal-iżvilupp tas-sistemi, inklużi sistemi ta' żvilupp, ittestjar, staging u preproduzzjoni

2.1.4 Komponenti open-source u ta' partijiet terzi integrati f'applikazzjonijiet interni

2.1.5 Software implimentat fuq il-post, f'ambjenti cloud privati, ibridi jew pubbliċi

2.2 L-utenti u l-entitajiet kollha li jipparteċipaw fl-iżvilupp, l-ittestjar jew l-implimentazzjoni tas-sistemi fil-kuntest organizzattiv huma soġġetti għal din il-politika, inklużi forniturі ta' servizzi ġestiti (MSPs) u forniturі ta' pjattaformi.

3. Objettivi

3.1 Għandhom jiġu integrati kontrolli tas-sigurtà fil-fażijiet kollha tal-iżvilupp ta' software, mid-disinn sat-tqegħid fis-servizz, biex it-tnaqqis tar-riskju jkun proattiv u kontinwu.

3.2 Għandha tiġi evitata l-introduzzjoni ta' vulnerabbiltajiet sfruttabbli bħal difetti ta' injection, awtentikazzjoni mhux sigura u espożizzjoni għal dgħufijiet magħrufa ta' partijiet terzi.

3.3 Għandhom jiġu stabbiliti u applikati prattiki ta' kodifikazzjoni sigura allinjati ma' OWASP, SANS CWE u linji gwida speċifiċi għall-qafas teknoloġiku.

3.4 Għandu jiġi żgurat li l-kodiċi kollu jgħaddi minn reviżjoni bejn il-pari, analiżi awtomatizzata u verifika tas-sigurtà qabel l-implimentazzjoni.

3.5 Għandhom jiġu mmaniġġjati r-riskji tal-iżvilupp li jirriżultaw minn attivitajiet esternalizzati, l-inklużjoni ta' kodiċi ta' partijiet terzi u l-użu mill-ġdid ta' software open-source.

3.6 Għandhom jiġu protetti l-ambjenti ta' żvilupp, ittestjar u staging minn aċċess mhux awtorizzat u għandu jiġi evitat l-użu ta' data tal-produzzjoni mingħajr masking jew anonimizzazzjoni approvati.

3.7 Għandu jiġi promoss l-għarfien dwar is-sigurtà fost l-iżviluppaturi, il-maniġers tal-prodott u l-professjonisti tal-assigurazzjoni tal-kwalità permezz ta' moduli ta' taħriġ ibbażati fuq ir-rwoli u aġġornamenti kontinwi dwar theddid emerġenti.

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 li r-rekwiżiti tal-iżvilupp sigur jiġu applikati madwar l-organizzazzjoni kollha.

4.1.2 Japprova standards ta' kodifikazzjoni sigura u ftehimiet ta' żvilupp ma' partijiet terzi.

4.1.3 Jivvalida deċiżjonijiet ta' trattament tar-riskju għal vulnerabbiltajiet mhux riżolti jew differiti.

4.2 Responsabbli għas-Sigurtà tal-Applikazzjonijiet / Maniġer DevSecOps

4.2.1 Jiżviluppa, iżomm u jippromwovi linji gwida ta’ kodifikazzjoni sigura.

4.2.2 Jintegra l-ittestjar statiku u dinamiku tas-sigurtà fil-pipelines ta’ CI/CD.

4.2.3 Jagħmel rieżamijiet tas-sigurtà tal-kodiċi u jiddefinixxi azzjonijiet ta’ rimedjazzjoni obbligatorji.

[... 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, jew aktar ta’ spiss b’reazzjoni għal:

9.1.1 Reviżjonijiet ewlenin fil-metodoloġiji tal-iżvilupp jew fl-għodod DevOps

9.1.2 Inċidenti materjali ta’ sigurtà li jirriżultaw minn vulnerabbiltajiet tal-applikazzjonijiet

9.1.3 Bidliet fir-rekwiżiti regolatorji relatati ma’ software sigur (eż. GDPR, DORA)

9.1.4 Standards ġodda tal-industrija jew intelligence dwar it-theddid (eż. OWASP Top 10, SLSA, MITRE CWE)

9.2 Ir-rieżami tal-politika għandu jitmexxa mir-Responsabbli għas-Sigurtà tal-Applikazzjonijiet b’koordinazzjoni mas-CISO, periti tas-software, tmexxija tal-QA u konsulent legali (għall-implikazzjonijiet ta’ kodiċi ta’ partijiet terzi).

9.3 Kwalunkwe reviżjoni għandha tiġi rreġistrata fir-Reġistru tal-Kontroll tad-Dokumenti tal-ISMS, titqiegħed taħt kontroll tal-verżjoni u tiġi kkomunikata lit-timijiet milquta permezz ta’ noti tar-rilaxx jew taħriġ obbligatorju.

9.4 Verżjonijiet legati għandhom jinżammu fir-repożitorju tal-arkivju għal traċċabbiltà legali u ta’ awditjar.

10. Politiki relatati u rabtiet

10.1 P1 – Politika tas-Sigurtà tal-Informazzjoni. Tistabbilixxi l-mandat strateġiku għall-integrazzjoni tas-sigurtà fis-sistemi tal-informazzjoni kollha, li minnhom l-iżvilupp sigur huwa kontroll operattiv fundamentali.

10.2 P4 – Politika dwar il-Kontroll tal-Aċċess. Tiddefinixxi l-miżuri ta’ kontroll għar-restrizzjoni tal-aċċess għal ambjenti ta’ żvilupp, repożitorji, għodod tal-build u pipelines ta’ CI/CD.

10.3 P5 – Politika tal-Ġestjoni tat-Tibdil. Tiżgura li bidliet fil-kodiċi, rilaxxi u implimentazzjonijiet ikunu soġġetti għal approvazzjoni xierqa, ippjanar tat-treġġigħ lura u verifika wara l-implimentazzjoni.

10.4 P12 – Politika tal-Ġestjoni tal-Assi. Tappoġġa l-inventarju tal-ambjenti ta’ żvilupp, repożitorji tas-sors u sistemi tal-build bħala assi ġestiti soġġetti għal klassifikazzjoni u protezzjoni.

10.5 P22 – Politika tal-Illoggjar u l-Monitoraġġ. Tapplika għall-pipelines tal-iżvilupp u tiżgura li l-proċessi tal-build, il-promozzjonijiet tal-kodiċi u l-avvenimenti tal-implimentazzjoni jiġu rreġistrati, monitorjati u analizzati għal anomaliji ta’ sigurtà.

10.6 P30 – Politika dwar ir-Rispons għall-Inċidenti. Tipprovdi l-qafas għall-analiżi u r-rispons għal difetti tas-sigurtà skoperti wara l-implimentazzjoni jew waqt l-ittestjar tas-sigurtà tal-applikazzjonijiet.

11. Standards u oqfsa ta’ referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 8.1 – Ippjanar u kontroll operattiv: Teħtieġ l-integrazzjoni ta’ proċessi u kontrolli ta’ żvilupp sigur fl-operazzjonijiet.

11.2 ISO/IEC 27002:2022 – Kontrolli 8.25–8.28

11.2.1 Kontroll 8.25 tal-Anness A – Ċiklu tal-ħajja tal-iżvilupp sigur: Jimponi l-inklużjoni formali tas-sigurtà fid-disinn u fl-iżvilupp tas-software.

11.2.2 Kontroll 8.26 tal-Anness A – Rekwiżiti tas-sigurtà tal-applikazzjonijiet: Jeħtieġ id-definizzjoni ta’ kodifikazzjoni sigura u kriterji ta’ aċċettazzjoni tas-sigurtà.

11.2.3 Kontroll 8.27 tal-Anness A – Arkitettura tas-sistema sigura u prinċipji tal-inġinerija: Jeħtieġ l-applikazzjoni ta' prinċipji ta' disinn tas-sigurtà u l-mitigazzjoni ta' dgħufijiet magħrufa.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-3 sa SA-15: Jistabbilixxi prattiki strutturati għall-iżvilupp tas-sigurtà tal-applikazzjonijiet, inklużi rekwiżiti għad-disinn, l-integrità tal-kodiċi u l-ittestjar.

11.3.2 SI-10 – Verifika tal-Input tal-Informazzjoni: Jindirizza d-difiżi tal-kodifikazzjoni sigura.

11.3.3 SR-3 – Protezzjoni tal-Katina tal-Provvista: Jeħtieġ verifika ta' software, komponenti u fornituri ta' żvilupp ta' partijiet terzi.

11.4 GDPR tal-UE (2016/679)

11.4.1 Artikolu 25 – Protezzjoni tad-Data mid-Disinn u b'Mod Predefinit: Jobbliga l-integrazzjoni tas-sigurtà u tal-privatezza fl-iżvilupp tas-sistemi.

11.4.2 Artikolu 32 – Sigurtà tal-Ipproċessar: Jappoġġa miżuri tekniċi bħall-verifika tal-input, kontrolli tal-aċċess u implimentazzjoni sigura.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikolu 21(2)(e–f): Jeħtieġ prattiki ta' żvilupp tas-software li jinkludu ġestjoni tal-vulnerabbiltajiet, sigurtà tal-kodiċi u rappurtar tal-inċidenti.

11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 9 – Ġestjoni tar-riskju tal-ICT: Jeħtieġ prattiki ta' żvilupp sigur għal entitajiet finanzjarji, inklużi kontrolli tal-kwalità tas-software u rimedjazzjoni tad-difetti.

11.6.2 Artikolu 10 – Kontinwità tan-negozju u ttestjar: Jinkoraġġixxi ttestjar rigoruż u verifika tas-sistemi tal-ICT, inklużi l-applikazzjonijiet.

11.7 COBIT 2019

11.7.1 BAI03 – Ġestjoni tal-Identifikazzjoni u l-Bini tas-Soluzzjonijiet: Tirregola d-disinn, l-iżvilupp u l-integrazzjoni tas-sigurtà f'soluzzjonijiet ġodda.

11.7.2 BAI07 – Ġestjoni tal-Aċċettazzjoni tat-Tibdil u t-Tranżizzjoni: Tiżgura implimentazzjoni sigura u evalwazzjoni wara l-implimentazzjoni.

11.7.3 DSS05 – Ġestjoni tas-Servizzi tas-Sigurtà: Tapplika l-verifika tas-sigurtà għall-provvista ta' software u servizzi.