					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P25					Titlu tad-dokument: **Politika dwar ir-Rekwiżiti tas-Sigurtà tal-Applikazzjonijiet**						
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	—
ISO/IEC 27002:2022	Kontrolli 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
GDPR tal-UE	Artikoli 25, 32	—
Direttiva NIS2 tal-UE	Artikoli 21(2)(f), 23	—
DORA tal-UE	Artikoli 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Għan

1.1 Din il-politika tiddefinixxi rekwiżiti obbligatorji tas-sigurtà fil-livell tal-applikazzjoni għal softwer żviluppat, akkwistat, integrat jew implimentat mill-organizzazzjoni. Tiżgura li l-applikazzjonijiet kollha jkunu mfassla, implimentati u miżmuma skont il-prinċipji ta’ żvilupp sigur, l-obbligi regolatorji u l-aptit għar-riskju tal-organizzazzjoni.

1.2 Din il-politika tirrikjedi l-integrazzjoni tas-sigurtà tul iċ-ċiklu tal-ħajja tal-applikazzjoni, inklużi l-awtentikazzjoni tal-utenti, il-prattiki ta’ ġestjoni tad-data, il-protezzjoni tal-interfaċċi u l-interazzjoni sigura ma’ APIs jew servizzi.

1.3 Permezz tal-adozzjoni ta’ din il-politika, l-organizzazzjoni għandha l-għan li tipprevjeni l-introduzzjoni ta’ vulnerabbiltajiet fis-softwer, tipproteġi data sensittiva u tiżgura t-traċċabbiltà u r-reżiljenza kontra exploit u abbuż.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għal dawn kollha:

2.1.1 applikazzjonijiet żviluppati internament jew akkwistati minn sorsi esterni, inklużi SaaS u għodod żviluppati apposta

2.1.2 applikazzjonijiet li jappoġġjaw operazzjonijiet kritiċi tan-negozju, aċċess tal-klijenti jew l-ipproċessar ta’ data rregolata

2.1.3 timijiet tal-iżvilupp, DevOps, assigurazzjoni tal-kwalità (QA), prodott u sigurtà

2.1.4 żviluppaturi ta’ partijiet terzi, fornituri tas-softwer u sħab ta’ integrazzjoni b’aċċess għal applikazzjonijiet tal-organizzazzjoni jew APIs

2.2 Tapplika fl-ambjenti kollha: żvilupp, ittestjar, staging, produzzjoni u rkupru minn diżastru, irrispettivament minn jekk humiex ospitati fuq il-post, f’ċentri tad-data privati jew f’ambjenti cloud pubbliċi.

3. Objettivi

3.1 Jiġu definiti rekwiżiti bażi tas-sigurtà, kemm funzjonali kif ukoll mhux funzjonali, li jridu jintlaħqu mill-applikazzjonijiet kollha, irrispettivament mill-metodu ta’ żvilupp jew mill-istack teknoloġiku.

3.2 Tiġi żgurata l-integrazzjoni ta’ kontrolli protettivi fil-livell tal-applikazzjoni, inklużi l-validazzjoni tal-input, il-kodifikazzjoni tal-output, il-ġestjoni tal-iżbalji u s-sigurtà tas-sessjonijiet.

3.3 Tkun obbligatorja l-implimentazzjoni sigura ta’ mekkaniżmi ta’ awtentikazzjoni, awtorizzazzjoni u kontroll tal-aċċess, allinjati mal-politiki tal-organizzazzjoni dwar l-identità u l-aċċess.

3.4 Tkun obbligatorja l-interazzjoni sigura ma’ APIs, interfaċċi tal-web u komponenti ta’ partijiet terzi bl-użu ta’ protokolli approvati u kontrolli tas-sigurtà.

3.5 Jitħalla possibbli s-sejbien bikri u l-mitigazzjoni tal-vulnerabbiltajiet permezz ta' analiżi statika u dinamika, rieżamijiet tal-kodiċi u immudellar tat-theddid.

3.6 Tiġi protetta data sensittiva f'konformità mar-rekwiżiti regolatorji billi jiġu infurzati l-iċċifrar, il-klassifikazzjoni u l-loġika taż-żamma tad-data.

3.7 Tkun żgurata verifika kontinwa tal-pożizzjoni tas-sigurtà tal-applikazzjoni wara l-implimentazzjoni, permezz ta' ttestjar, monitoraġġ u l-kapaċità li tintwera l-konformità.

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 l-allinjament tagħha mal-istrateġija tas-sigurtà tal-informazzjoni u mal-pożizzjoni tar-riskju tal-organizzazzjoni.

4.1.2 Japprova r-rekwiżiti tas-sigurtà tal-applikazzjonijiet u jiżgura l-applikazzjoni ta' kontrolli obbligatorji fil-funzjonijiet tal-iżvilupp u tal-akkwist.

4.2 Responsabbli għas-Sigurtà tal-Applikazzjonijiet / Maniġer DevSecOps

4.2.1 Jiddefinixxi kontrolli bażi tas-sigurtà u metodoloġiji ta' ttestjar għall-komponenti tal-applikazzjoni.

4.2.2 Jeżerċita sorveljanza fuq l-integrazzjoni sigura ta' għodod bħal SAST, DAST, IAST u SCA fil-pipeline tat-twassil tas-softwer.

4.2.3 Iżomm il-Lista ta' Kontroll tar-Rekwiżiti tas-Sigurtà tal-Applikazzjonijiet u l-kriterji ta' verifika.

[... 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 żvelar ta' vulnerabbiltajiet kritiċi li jaffettwaw oqfsa jew dipendenzi komuni

9.1.2 aġġornamenti għall-obbligi regolatorji dwar is-sigurtà tal-applikazzjonijiet (eż. NIS2, DORA)

9.1.3 bidliet maġġuri fil-prattiki tal-iżvilupp tas-softwer, fl-għodod jew fl-arkitettura cloud tal-organizzazzjoni

9.1.4 sejbiet minn awditi interni jew testijiet ta' penetrazzjoni esterni

9.2 Ir-rieżami għandu jitmexxa mir-Responsabbli għas-Sigurtà tal-Applikazzjonijiet, f'koordinazzjoni mas-CISO, l-inġinerija DevOps, il-funzjoni Legali, l-Akkwist u r-responsabbli tal-QA.

9.3 Ir-reviżjonijiet kollha għandhom ikunu taħt kontroll tal-verżjoni fir-Reġistru tal-Kontroll tad-Dokumenti tal-ISMS u mqassma lit-timijiet kollha tal-iżvilupp u tal-prodott affettwati.

9.4 Verżjonijiet sostitwiti għandhom jiġu arkivjati għal mhux inqas minn tliet snin biex tiġi żgurata t-traċċabbiltà, l-awditabbiltà u l-appoġġ għall-investigazzjoni ta' ksur.

10. Politiki relatati u rabtiet

10.1 P1 – Politika tas-Sigurtà tal-Informazzjoni. Tistabbilixxi l-bażi għall-protezzjoni tas-sistemi u tad-data, li taħtha huma meħtieġa kontrolli fil-livell tal-applikazzjoni biex jipprevjenu aċċess mhux awtorizzat, tnixxija ta' data u exploit.

10.2 P4 – Politika dwar il-Kontroll tal-Aċċess. Tiddefinixxi l-istandards tal-ġestjoni tal-identità u tas-sessjonijiet li għandhom jiġu applikati mill-applikazzjonijiet kollha, inklużi awtentikazzjoni b'saħħitha, l-inqas privileġġ u rekwiżiti ta' rieżami tal-aċċess.

10.3 P5 – Politika tal-Ġestjoni tat-Tibdil. Tirregola l-promozzjoni tal-kodiċi u tal-konfigurazzjonijiet tal-applikazzjoni lejn ambjenti ta' produzzjoni, filwaqt li tiżgura li bidliet mhux awtorizzati jew mhux ittestjati jiġu mblukkati.

10.4 P17 – Politika dwar il-Protezzjoni tad-Data u l-Privatezza. Tirrikjedi li l-applikazzjonijiet jimplimentaw privatezza mid-disinn u jiżguraw il-ġestjoni legali, l-iċċifrar u ż-żamma ta' data personali u sensittiva fl-ambjenti kollha.

10.5 P24 – Politika dwar l-Iżvilupp Sigur. Tipprovdi l-qafas usa' għall-integrazzjoni tas-sigurtà fis-SDLC, li fih din il-politika tiddefinixxi r-rekwiżiti konkreti u l-kontrolli tekniċi li għandhom jiġu implimentati fil-livell tal-applikazzjoni.

10.6 P30 – Politika dwar ir-Rispons għall-Inċidenti. Tobbliga l-ġestjoni strutturata ta' inċidenti tas-sigurtà tal-applikazzjonijiet, inklużi vulnerabbiltajiet identifikati wara l-implimentazzjoni jew waqt ittestjar ta' penetrazzjoni, u tiddeskrivi proċeduri ta' eskalazzjoni, trażżin u rkupru.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001:2022

11.1.1 Klawżola 8.1 – Ippjanar u Kontroll Operattiv: Tirrikjedi li s-sigurtà tal-applikazzjonijiet tkun integrata fil-proċessi u fis-sistemi biex jiġu żgurati l-Kunfidenzjalità, l-Integrità u d-Disponibbiltà (CIA).

11.2 ISO/IEC 27002:2022

11.2.1 Kontrolli 8.25–8.26: Jiddettaljaw l-aspettattivi għas-sigurtà fil-livell tal-applikazzjoni, inklużi Prattiki ta' Kodifikazzjoni Sigura, immudellar tat-theddid, kontrolli arkitettoniċi u verifika ta' softwer ta' partijiet terzi.

11.2.2 Kontroll tal-Anness A 8.25 – Ċiklu tal-ħajja tal-iżvilupp sigur: Jeħtieġ l-integrazzjoni tas-sigurtà tul iċ-ċiklu tal-ħajja tal-applikazzjoni.

11.2.3 Kontroll tal-Anness A 8.26 – Rekwiżiti tas-Sigurtà tal-Applikazzjonijiet: Jagħmel obbligatorja d-definizzjoni u l-applikazzjoni ta' kontrolli tekniċi biex jipproteġu l-applikazzjonijiet kontra użu ħażin u kompromess.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Ittestjar u Valutazzjoni tas-Sigurtà mill-Iżviluppatur: Jagħmel obbligatorji l-analiżi statika, dinamika u t-testijiet ta' penetrazzjoni waqt l-iżvilupp.

11.3.2 SA-15 – Proċess, Standards u Għodod tal-Iżvilupp: Jistabbilixxi standards formali għall-iżvilupp sigur tal-applikazzjonijiet.

11.3.3 SI-10 – Validazzjoni tal-Input tal-Informazzjoni: Tirrikjedi mekkaniżmi ta' kontroll għall-prevenzjoni ta' attakki ta' injection u parsing.

11.4 GDPR tal-UE (2016/679)

11.4.1 Artikolu 25 – Protezzjoni tad-Data mid-Disinn u b'Mod Predefinit: Jeħtieġ l-integrazzjoni tal-protezzjoni tad-data u tal-privatezza fil-loġika tal-applikazzjoni u fil-flussi tax-xogħol.

11.4.2 Artikolu 32 – Sigurtà tal-Ipproċessar: Jagħmel obbligatorja l-adozzjoni ta' miżuri tekniċi xierqa, bħall-validazzjoni tal-input, l-iċċifrar u kontrolli siguri tal-aċċess.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikolu 21(2)(f): Jeħtieġ prattiki għall-ġestjoni tal-vulnerabbiltajiet u għaċ-ċiklu tal-ħajja sigur tal-applikazzjoni għal entitajiet essenzjali u importanti.

11.5.2 Artikolu 23 – Rappurtar ta' Inċidenti tas-Sigurtà: Jeħtieġ kapaċitajiet ta' logging u monitoraġġ fil-livell tal-applikazzjoni biex jinstabu u jiġu rrappurtati inċidenti sinifikanti.

11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 9 – ġestjoni tar-riskju tal-ICT: Jobbliga lill-entitajiet finanzjarji jiżguraw li l-applikazzjonijiet ikunu siguri, ittestjati u reżiljenti għat-theddid ċibernetiku.

11.6.2 Artikolu 11 – Ittestjar tal-Għodod tal-ICT: Jinkoraġġixxi testijiet perjodiċi ta' penetrazzjoni u eżerċizzji ta' red team fuq applikazzjonijiet u servizzi kritiċi.

11.7 COBIT 2019

11.7.1 BAI03 – Manage Solutions Identification and Build: Jistabbilixxi rekwiżiti ta' disinn u kontroll waqt l-iżvilupp tal-applikazzjonijiet.

11.7.2 BAI09 – Manage Applications: Jenfasizza l-manutenzjoni sigura, il-monitoraġġ u t-titjib ta' applikazzjonijiet operattivi.

11.7.3 DSS05 – Manage Security Services: Jorbot il-protezzjoni tal-applikazzjonijiet mal-operazzjonijiet u l-kontrolli usa' tas-sigurtà tal-organizzazzjoni.