					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P25S					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	Kontrolli operattivi, inkluża s-sigurtà tal-applikazzjonijiet
ISO/IEC 27002:2022	Kontrolli 8.25–8.26	Disinn sigur, żvilupp sigur, ittestjar u reviżjoni tal-kodiċi
NIST SP 800-53 Rev.5	SA-11, SI-10	Ittestjar mill-iżviluppatur/tal-applikazzjoni, analiżi tal-kodiċi u prevenzjoni ta' difetti
GDPR tal-UE	Artikolu 25	Protezzjoni tad-data mid-disinn u b'mod awtomatiku
Direttiva NIS2 tal-UE	Artikolu 21(2)(a), (e)	Miżuri tekniċi biex jiżguraw is-sigurtà tal-applikazzjonijiet u jidentifikaw ir-riskji
DORA tal-UE	Artikoli 9(2)(c), 10(2)(c)	Sigurtà tal-applikazzjonijiet għar-reżiljenza operattiva diġitali
COBIT 2019	BAI03	Ġestjoni tal-iżvilupp/akkwist ta' software sigur

1. Għan

1.1 Din il-politika tiddefinixxi l-kontrolli minimi u obbligatorji tas-sigurtà tal-applikazzjonijiet meħtieġa għas-software u s-soluzzjonijiet ta' sistemi kollha użati mill-organizzazzjoni, irrispettivament minn jekk humiex żviluppati internament jew akkwistati minn fornituri esterni.

1.2 Din tiżgura li l-applikazzjonijiet ikunu mfassla, implimentati u miżmuma b'mod li jipproteġi d-data tal-klijenti, tal-impjegati u tan-negozju minn aċċess mhux awtorizzat, użu ħażin, alterazzjoni jew qerda.

1.3 Din il-politika tappoġġa l-isforzi tal-organizzazzjoni biex tikseb u żżomm iċ-ċertifikazzjoni ISO/IEC 27001, tissodisfa l-obbligi tal-GDPR u tan-NIS2, u tnaqqas ir-riskji operattivi marbuta ma' implimentazzjonijiet ta' software mhux sigur.

1.4 Tgħin biex jiġi stabbilit approċċ konsistenti u awditabbli għas-sigurtà tal-applikazzjonijiet għall-SMEs billi tistabbilixxi checklist uniformi ta' karatteristiċi u prattiki ta' sigurtà, adattata għal ambjenti b'riżorsi tekniċi interni limitati.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għall-applikazzjonijiet, is-sistemi, l-għodod u l-pjattaformi kollha li:

2.1.1 Jiġu żviluppati internament, personalizzati jew skriptjati għal użu intern

2.1.2 Jinxtraw bħala software kummerċjali, SaaS jew sistemi f'ambjent cloud

2.1.3 Jipproċessaw, jaħżnu jew jittrażmettu data personali, reġistri tan-negozju jew informazzjoni operattiva sensittiva

2.1.4 Ikunu aċċessati minn impjegati, kuntratturi, klijenti jew sħab permezz ta' netwerks interni, l-internet jew pjattaformi mobbli

2.2 Il-politika tkopri:

2.2.1 Żviluppaturi (interni jew ikkuntrattati)

2.2.2 Fornituri tas-software u fornituri ta' servizzi cloud

2.2.3 Persunal ta' appoġġ tal-IT jew amministraturi responsabbli mit-tqegħid fis-servizz u l-appoġġ

2.2.4 Sidien tal-applikazzjonijiet u utenti tan-negozju involuti fl-approvazzjoni u s-sorveljanza tas-sistema

3. Objettivi

3.1 Jiġi żgurat li l-applikazzjonijiet kollha użati mill-organizzazzjoni jkollhom kontrolli tas-sigurtà integrati u verifikabbli li jimmitigaw vulnerabbiltajiet komuni tas-software.

3.2 Tiġi protetta l-Kunfidenzjalità, l-Integrità u d-Disponibbiltà (CIA) tad-data pproċessata mill-applikazzjonijiet, irrispettivament minn fejn ikunu ospitati.

3.3 Jiġi impost ittestjar, rieżami u verifika formali tas-sigurtà tal-applikazzjonijiet qabel ma kwalunkwe applikazzjoni ġdida jew aġġornament ewlieni jiġi approvat għall-użu fl-ambjent ta' produzzjoni.

3.4 Jiġi żgurat immaniġġjar konsistenti u sigur tal-kredenzjali tal-utent, tad-data tas-sessjoni u tad-drittijiet ta' aċċess fis-sistemi kollha kritiċi għan-negozju.

3.5 Jiġu imposti reġistrazzjoni tal-awditjar, kapaċitajiet ta' awditjar u karatteristiċi ta' monitoraġġ fl-applikazzjonijiet kollha biex jappoġġaw is-sejbien u r-rispons għal attività suspettuża.

3.6 Jitnaqqsu r-riskji legali u ta' konformità billi jiġi żgurat li l-applikazzjonijiet jissodisfaw ir-rekwiżiti regolatorji ta' sigurtà applikabbli.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Iġorr ir-responsabbiltà ġenerali għas-sigurtà tal-applikazzjonijiet fl-organizzazzjoni kollha.

4.1.2 Japprova din il-politika u jiżgura li l-akkwisti jew il-proġetti ta' żvilupp kollha jkunu konformi magħha.

4.1.3 Jiżgura li l-forniturі u l-forniturі tas-servizzi jkunu marbuta kuntrattwalment mar-rekwiżiti tas-sigurtà tal-applikazzjonijiet.

4.1.4 Jirrieżamina u japprova eċċezzjonijiet għar-riskju fejn il-konformità sħiħa ma tistax tintlaħaq minħabba limitazzjonijiet tan-negozju.

4.2 Sid tal-Applikazzjoni (jekk maħtur)

4.2.1 Jidentifika l-ħtiġijiet speċifiċi tas-sigurtà tal-applikazzjoni waqt l-għażla tas-sistema jew il-bidu tal-proġett.

4.2.2 Jivverifika li karatteristiċi ewlenin bħall-protezzjoni tal-login, l-iċċifrar u r-reġistri tal-attività jkunu inklużi.

4.2.3 Jieħu sehem fir-rieżamijiet tar-riskju qabel l-implimentazzjoni u jikkonferma li l-kontrolli tas-sigurtà jissodisfaw il-ħtiġijiet tan-negozju.

[... 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-Maniġer Ġenerali mill-inqas darba kull sena kalendarja biex:

9.1.1 Tirrifletti bidliet fir-rekwiżiti regolatorji (eż. GDPR, NIS2, DORA)

9.1.2 Tinkorpora theddid u tekniki ta' attakk ġodda jew emerġenti

9.1.3 Taġġorna l-lingwa u r-rekwiżiti biex jirriflettu bidliet fil-pjattaformi, il-forniturі jew il-metodi ta' żvilupp

9.2 Għandhom isiru wkoll rieżamijiet interim meta:

9.2.1 Jiġu introdotti applikazzjonijiet ġodda

9.2.2 Applikazzjonijiet eżistenti jgħaddu minn aġġornamenti sinifikanti jew integrazzjoni

9.2.3 Iseħħ inċident jew ksur relatat ma' applikazzjoni

9.2.4 Jiġu identifikati riskji ġodda minn avviżi esterni jew twissijiet tal-industrija

9.3 L-aġġornamenti kollha għal din il-politika għandhom:

9.3.1 Jiġu approvati mill-Maniġer Ġenerali

9.3.2 Ikunu dokumentati bl-istorja tal-verżjonijiet u r-raġuni għat-tibdil

9.3.3 Jiġu kkomunikati lill-impjegati, lill-iżviluppaturi u lill-fornituri kollha involuti fil-ġestjoni tal-applikazzjonijiet

9.3.4 Jinħażnu b'mod sigur għal referenza ta' awditjar u konformità

10. Politiki relatati u rabtiet

10.1 Din il-politika hija appoġġata direttament minn u tikkontribwixxi għall-applikazzjoni tal-politiki tas-sigurtà allinjati mal-SME li ġejjin:

10.1.1 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tassenja r-responsabbiltà għall-approvazzjoni tal-applikazzjonijiet, l-infurzar tal-politika u l-ġestjoni tal-fornituri.

10.1.2 P4S – Politika dwar il-Kontroll tal-Aċċess: Tiżgura li l-aċċess għall-applikazzjonijiet ikun allinjat mal-prinċipji tal-inqas privileġġ u tal-kontroll tas-sessjoni.

10.1.3 P8S – Politika dwar l-Għarfien tas-Sigurtà tal-Informazzjoni u t-Taħriġ: Tiżgura li l-utenti u l-iżviluppaturi jkunu mħarrġa biex jagħrfu u jirrappurtaw theddid relatat mal-applikazzjonijiet.

10.1.4 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tipprovdi salvagwardji tal-privatezza tad-data li għandhom jiġu applikati minn kwalunkwe applikazzjoni li tipproċessa informazzjoni personali.

10.1.5 P14S – Politika ta' Żamma u Rimi tad-Data: Tirregola kif reġistri, backups u data sensittiva ġġenerati mill-applikazzjonijiet għandhom jinżammu, jiġu arkivjati u jinqerdu b'mod sigur.

10.1.6 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiddeskrivi l-passi għall-identifikazzjoni, ir-rappurtar u t-trażżin ta' avvenimenti tas-sigurtà relatati mal-applikazzjonijiet.

10.2 Flimkien, dawn il-politiki jiżguraw li s-sigurtà tal-applikazzjonijiet tkun integrata bis-sħiħ fis-Sistema ta' Ġestjoni tas-Sigurtà tal-Informazzjoni (ISMS) tal-organizzazzjoni u lesta għall-awditjar.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 8.1 – Teħtieġ li l-organizzazzjonijiet jistabbilixxu kontrolli operattivi biex jindirizzaw riskji tas-sigurtà tal-informazzjoni, inklużi dawk relatati mal-applikazzjonijiet u s-sistemi tas-software.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.25 – Jagħti gwida biex jiġu implimentati prattiki ta' disinn sigur, żvilupp sigur u reviżjoni tal-kodiċi fl-applikazzjonijiet kollha, inklużi dawk ipprovduti mill-fornituri.

11.2.2 Kontroll 8.26 – Jirrakkomanda ittestjar formali tal-kontrolli tas-sigurtà tal-applikazzjonijiet, b'mod partikolari f'oqsma li jinvolvu kontroll tal-aċċess, validazzjoni tal-input u ġestjoni tas-sessjoni.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Jispeċifika rekwiżiti għall-ittestjar mill-iżviluppatur, l-analiżi tal-kodiċi u skannjar dinamiku tal-applikazzjonijiet qabel it-tqegħid fis-servizz.

11.3.2 SI-10 – Jindirizza s-sejbien u l-prevenzjoni ta' difetti komuni tas-software, b'enfasi fuq l-għarfien tal-iżviluppaturi u s-salvagwardji tekniċi.

11.4 GDPR tal-UE (2016/679)

11.4.1 Artikolu 25 – "Il-protezzjoni tad-data mid-disinn u b'mod awtomatiku" jobbliga li l-privatezza u s-sigurtà jiġu integrati fid-disinn ewlieni tal-applikazzjonijiet li jimmaniġġjaw data personali.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikolu 21(2)(a) u (e) – Teħtieġ li entitajiet essenzjali u importanti jimplimentaw miżuri tekniċi biex jiżguraw is-sigurtà tal-applikazzjonijiet u jidentifikaw riskji relatati mas-software.

11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 9(2)(c), 10(2)(c) – Teħtieġ li SMEs tas-settur finanzjarju jintegraw kontrolli tas-sigurtà fil-livell tal-applikazzjoni u jwettqu valutazzjonijiet regolari biex iżommu r-reżiljenza operattiva diġitali.

11.7 COBIT 2019

11.7.1 BAI03 – “Manage Solutions Identification and Build” jiggwida l-iżvilupp jew l-akkwist ta’ software sigur allinjat mar-riskju, mal-konformità u mar-rekwiżiti tan-negozju, anke f’ambjenti ta’ SMEs b’riżorsi limitati.