					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P26S					Titlu tad-dokument: **Politika dwar is-Sigurtà ta' Partijiet Terzi u l-Forniturі**						
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 mal-istandards u r-regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	Kontrolli operattivi għar-relazzjonijiet ma' partijiet terzi u fornituri
ISO/IEC 27002:2022	Kontrolli 5.19–5.22	Kontrolli tas-sigurtà tal-fornituri, termini kuntrattwali tas-sigurtà, ġestjoni tat-tibdil, monitoraġġ u rieżami
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Akkwist, konfigurazzjoni, ftehimiet ta' interkonnessjoni u kontrolli għall-persunal estern
GDPR tal-UE	Artikoli 28, 32	Ftehimiet dwar l-ipproċessar tad-data, rekwiżiti ta' sigurtà għall-proċessuri
Direttiva NIS2 tal-UE	Artikoli 21(2)(a)(b)(i), 23(1)	Ġestjoni tar-riskju tal-katina tal-provvista, sorveljanza tas-servizzi ta' partijiet terzi
DORA tal-UE	Artikoli 5(1)(2), 28(1)(2)	Ġestjoni tar-riskju tal-ICT għal fornituri terzi ta' servizzi
COBIT 2019	APO10, APO12, DSS05	Ġestjoni tal-fornituri u integrazzjoni tar-riskju

1. Għan

1.1 Din il-politika tistabbilixxi r-rekwiżiti obbligatorji tas-sigurtà għall-ingaġġ, il-ġestjoni u t-terminazzjoni ta' relazzjonijiet ma' partijiet terzi u fornituri li jaċċessaw jew jinfluwenzaw id-data, is-sistemi jew is-servizzi tal-organizzazzjoni.

1.2 Tiżgura li fornituri esterni — inklużi fornituri ta' appoġġ tal-IT, operaturi ta' servizzi cloud, żviluppaturi tas-software u kuntratturi tal-proċessi tan-negozju — jimmaniġġjaw l-assi tal-kumpanija b'mod sigur u f'konformità mal-liġijiet u l-istandards applikabbli.

1.3 Din il-politika tnaqqas riskji bħal tnixxijiet tad-data, bidliet mhux awtorizzati fis-sistemi, multi regolatorji jew interruzzjonijiet fin-negozju kkawżati minn arranġamenti ma' partijiet terzi li ma jkunux siguri jew li ma jkunux governati kif xieraq.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għall-partijiet terzi kollha li:

2.1.1 Jipprovdu software, infrastruttura, hosting jew servizzi cloud

2.1.2 Jaċċessaw jew jimmaniġġjaw sistemi, apparat jew applikazzjonijiet interni

2.1.3 Jimmaniġġjaw data, dokumenti jew backups tal-kumpanija

2.1.4 Jappoġġjaw operazzjonijiet tan-negozju, riżorsi umani, finanzi jew servizzi lill-klijenti

2.2 Tapplika wkoll għal:

2.2.1 Persunal intern involut fl-għażla, l-ingaġġ jew is-sorveljanza tal-fornituri

2.2.2 Kull persunal li jimmaniġġja l-inklużjoni inizjali tal-fornituri, kuntratti, aċċess jew rieżamijiet

2.2.3 Kull sistema jew proċess li jiddependi fuq komponenti jew servizzi ta' partijiet terzi

3. Objettivi

3.1 Jiġi żgurat li l-forniturі kollha jissodisfaw aspettattivi tas-sigurtà definiti b'mod ċar.

3.2 Jiġi impost li l-kuntratti tal-forniturі jinkludu obbligi infurzabbli dwar is-sigurtà, il-privatezza u r-rispons għall-inċidenti.

3.3 Jiġu evalwati u dokumentati r-riskji tal-forniturі qabel ma jiġu ffirmati l-ftehimiet jew jingħata l-aċċess.

3.4 Jiġu applikati rieżamijiet regolari għal forniturі kritiċi jew ta' riskju għoli sabiex tiġi kkonfermata l-konformità.

3.5 Jiġi stabbilit proċess formali għall-eċċezzjonijiet, il-ġestjoni tal-inċidenti u l-aġġornamenti tal-kuntratti.

3.6 Tiġi appoġġjata l-konformità mal-obbligi ta' ISO/IEC 27001:2022, GDPR, NIS2 u DORA relatati mal-governanza tal-forniturі.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Għandu r-responsabbiltà aħħarija għall-għażla tal-forniturі u l-konformità tas-sigurtà

4.1.2 Japprova kuntratti, eċċezzjonijiet u eskalazzjonijiet li jinvolvu forniturі

4.1.3 Jissorvelja r-rispons għall-inċidenti u t-teħid tad-deċiżjonijiet meta forniturі jonqsu milli jissodisfaw l-obbligi tagħhom

4.2 Fornitur ta' Appoġġ tal-IT jew kuntatt intern għas-sigurtà

4.2.1 Jevalwa l-aċċess tekniku mitlub mill-forniturі

4.2.2 Jimplimenta regoli ta' kontroll tal-aċċess, jirrieżamina l-logs u jivverifika l-ġestjoni sigura tad-data

4.2.3 Jirrieżamina evidenza tal-kontrolli tas-sigurtà, ċertifikazzjonijiet jew riżultati tal-awditjar, fejn applikabbli

[... 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 trid tiġi rieżaminata mill-inqas darba fis-sena mill-Maniġer Ġenerali, bil-parteċipazzjoni tal-fornitur ta' appoġġ tal-IT jew tal-maniġer tal-forniturі.

9.2 Il-politika trid tiġi rieżaminata wkoll:

9.2.1 Wara kwalunkwe bidla sinifikanti fl-obbligi legali, regolatorji jew kuntrattwali

9.2.2 Wara kwalunkwe inċident tas-sigurtà tal-informazzjoni relatat ma' fornitur jew sejba tal-awditjar

9.2.3 Meta jiddaħħlu kategoriji ġodda ta' forniturі (eż. pjattaformi SaaS kritiċi)

9.3 L-aġġornamenti kollha jridu jkunu:

9.3.1 Dokumentati bl-istorja tal-verżjonijiet u r-raġuni tagħhom

9.3.2 Approvati mill-Maniġer Ġenerali

9.3.3 Ikkomunikati lill-persunal intern rilevanti u lill-maniġers tal-forniturі

9.3.4 Maħżuna mal-verżjonijiet preċedenti skont il-P14S – Politika ta' Żamma u Rimi tad-Data

10. Politiki relatati u rabtiet

10.1 L-effettività ta' din il-politika tiddependi fuq koordinazzjoni mal-politiki li ġejjin dwar is-sigurtà tal-informazzjoni għall-SMEs:

10.1.1 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tassenja r-responsabbiltà għas-sorveljanza tal-forniturі u l-infurzar tal-kuntratti.

10.1.2 P4S – Politika dwar il-Kontroll tal-Aċċess: Tipprovdi regoli għar-restrizzjoni tal-aċċess li jridu jiġu applikati meta l-forniturі jingħataw aċċess għas-sistema.

10.1.3 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tiżgura li l-forniturі li jimmaniġġjaw data personali josservaw il-prinċipji tal-protezzjoni tad-data u r-rekwiżiti legali.

10.1.4 P14S – Politika ta' Żamma u Rimi tad-Data: Tapplika għal kull data jew reġistru kondiviż ma' fornituri jew maħżun minnhom u tirregola r-rimi sigur wara t-terminazzjoni tal-kuntratt.

10.1.5 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiddeskrivi kif għandu jsir ir-rispons meta fornitur jikkawża jew ikun involut f'inċident ta' sigurtà, inklużi l-proċeduri ta' eskalazzjoni u l-ġestjoni tal-evidenza.

10.2 Dawn il-politiki jaħdmu flimkien biex jiżguraw li r-riskju tal-fornituri jkun ikkontrollat tul iċ-ċiklu tal-ħajja tal-kuntratt.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 8.1 – Teħtieġ l-implimentazzjoni ta' kontrolli operattivi, inklużi dawk applikati għal relazzjonijiet ma' partijiet terzi u fornituri.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.19 – Jiżgura li l-miżuri tas-sigurtà tal-fornituri jkunu allinjati mar-rekwiżiti tal-organizzazzjoni.

11.2.2 Kontroll 5.20 – Jeħtieġ ftehimiet formali li jkopru t-termini tas-sigurtà, ir-responsabbiltajiet u l-obbligi f'każ ta' ksur.

11.2.3 Kontroll 5.21 – Jikkontrolla bidliet fis-servizzi tal-fornituri li jistgħu jaffettwaw il-pożizzjoni tas-sigurtà.

11.2.4 Kontroll 5.22 – Jeħtieġ monitoraġġ u rieżami tas-servizzi tal-fornituri u tal-konformità tagħhom.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Jirregola l-akkwist ta' sistemi u servizzi esterni, u jeħtieġ evalwazzjonijiet tar-riskju u aspettattivi definiti.

11.3.2 SA-10 – Jikkontrolla l-konfigurazzjoni u l-proċeduri tat-tibdil li jinvolvu sistemi mmaniġġjati minn partijiet terzi.

11.3.3 CA-3 – Jeħtieġ ftehimiet ta' interkonnessjoni għal sistemi li jinvolvu entitajiet esterni.

11.3.4 PS-7 – Jispeċifika l-iskrining u r-responsabbiltà għall-persunal estern.

11.4 GDPR tal-UE (2016/679)

11.4.1 Artikolu 28 – Jeħtieġ ftehimiet dwar l-ipproċessar tad-data ma' fornituri li jaġixxu bħala proċessuri.

11.4.2 Artikolu 32 – Jobbliga miżuri tekniċi u organizzattivi (TOMs) xierqa ta' sigurtà għall-proċessuri tad-data kollha.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikolu 21(2)(a), (b), (i) – Jobbliga ġestjoni tar-riskju tal-katina tal-provvista tal-ICT u kontrolli għal partijiet terzi.

11.5.2 Artikolu 23(1) – Jeħtieġ sorveljanza dokumentata tas-servizzi ta' partijiet terzi għal entitajiet essenzjali u importanti.

11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 5(1) – Jeħtieġ qafas ta' ġestjoni tar-riskju tal-ICT li jkopri l-fornituri terzi kritiċi kollha.

11.6.2 Artikolu 5(2) – Jistabbilixxi kontrolli kuntrattwali u operattivi għad-dipendenzi fuq servizzi tal-ICT.

11.6.3 Artikolu 28(1), (2) – Jistabbilixxi regoli ta' sorveljanza għar-riskju tal-ICT minn partijiet terzi fis-settur finanzjarju.

11.7 COBIT 2019

11.7.1 APO10 – "Manage Suppliers" jiddeskrivi l-kontrolli tas-sourcing u l-aspettattivi għall-ġestjoni tar-relazzjonijiet.

11.7.2 APO12 – "Manage Risk" jintegra r-riskju tal-forniturifil-governanza tar-riskju tal-organizzazzjoni.

11.7.3 DSS05 – "Manage Security Services" japplika għal forniturigestiti ta' servizzi ta' partijiet terzi u forniturie sternalizzati ta' servizzi.