					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P26					Titlu tad-dokument: **Politika tas-Sigurtà ta' Partijiet Terzi u tal-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 ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	Ippjanar u Kontroll Operattiv: Jeħtieġ kontrolli formali fuq servizzi ta’ partijiet terzi li jaffettwaw l-ISMS
ISO/IEC 27002:2022	Kontrolli 5.19–5.22	Politiki u Proċeduri għar-Relazzjonijiet mal-Fornituri; Ġestjoni tar-Riskju tal-Fornituri; Ġestjoni tat-Twassil tas-Servizzi tal-Fornituri; Monitoraġġ u Rieżami tal-Fornituri
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Servizzi ta’ Sistemi Esterni; Ġestjoni tal-Konfigurazzjoni mill-Iżviluppatur; Interkonnessjonijiet tas-Sistemi; Sigurtà tal-Persunal ta’ Partijiet Terzi
GDPR tal-UE	Artikoli 28, 32, 33	Obbligi tal-proċessur, Sigurtà tal-ipproċessar, Notifika ta’ ksur ta’ data personali
Direttiva NIS2 tal-UE	Artikolu 21(2)(e–f)	Ġestjoni tal-fornituri bbażata fuq ir-riskju u sorveljanza tas-sigurtà
DORA tal-UE	Artikoli 28, 30	Riskju tal-ICT minn Partijiet Terzi, sorveljanza fuq Fornituri Kritiċi ta’ Partijiet Terzi tal-ICT
COBIT 2019	BAI05, DSS02, MEA03	Ġestjoni tal-Abilitazzjoni tat-Tibdil Organizzattiv; Ġestjoni tat-Talbiet għas-Servizz u l-Inċidenti; Monitoraġġ, Evalwazzjoni u Valutazzjoni tal-Konformità

1. Għan

1.1 Din il-politika tiddefinixxi r-rekwiżiti tas-sigurtà tal-informazzjoni għall-istabbiliment, il-ġestjoni u ż-żamma ta’ relazzjonijiet siguri ma’ fornituri u fornituri ta’ servizzi ta’ partijiet terzi.

1.2 Din tiżgura li l-fornituri kollha b’aċċess għad-data, is-sistemi jew l-infrastruttura tal-organizzazzjoni jkunu soġġetti għal kontrolli tas-sigurtà rigoruż, salvagwardji kuntrattwali u sorveljanza kontinwa matul iċ-ċiklu tal-ħajja tas-servizz.

1.3 Il-politika tappoġġa l-Kontrolli 5.19 sa 5.22 tal-Anness A ta’ ISO/IEC 27001 billi tintegra rekwiżiti tas-sigurtà fl-akkwist, fl-onboarding, fid-diliġenza dovuta, fil-ġestjoni tal-kuntratti, fil-monitoraġġ tas-servizzi u fil-proċessi ta’ terminazzjoni.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 Il-fornituri kollha ta’ partijiet terzi, il-kuntratturi, il-fornituri cloud u l-organizzazzjonijiet tas-servizzi li jipproċessaw jew jaċċessaw assi tal-informazzjoni tal-organizzazzjoni

2.1.2 Ir-rwoli interni kollha involuti fl-evalwazzjoni tal-forniturі, fl-onboarding, fil-kuntrattar, fil-ġestjoni tar-riskju, fil-monitoraġġ jew fit-terminazzjoni

2.1.3 Ir-relazzjonijiet kollha mal-forniturі li jinkludu aċċess għal data sensittiva, integrazzjoni ma' servizzi ta' produzzjoni jew appoġġ għal funzjonijiet kritiċi tan-negozju

2.2 Din tkopri kemm il-forniturі diretti kif ukoll is-subkuntratturi tagħhom fejn applikabbli, u tinkludi softwer, infrastruttura, appoġġ u servizzi ġestiti minn partijiet terzi.

3. Objettivi

3.1 Tiżgura li r-riskji tas-sigurtà relatati mal-forniturі jiġu identifikati, evalwati u mitigati b'mod konsistenti matul iċ-ċiklu tal-ħajja tar-relazzjoni.

3.2 Tintegra rekwiżiti standardizzati tas-sigurtà fil-kuntratti kollha mal-forniturі, inklużi obbligi ta' notifika ta' ksur, klawżoli ta' drittijiet ta' awditjar u responsabbiltajiet dwar il-protezzjoni tad-data.

3.3 Tirrikjedi diliġenza dovuta formali u evalwazzjonijiet tar-riskju dokumentati qabel ma jiġu ingaġġati forniturі ġodda jew jiġġeddu ftehimiet ta' servizz ta' riskju għoli.

3.4 Tistabbilixxi mekkaniżmi għall-monitoraġġ kontinwu tal-konformità tal-forniturі, inklużi rieżamijiet tal-prestazzjoni, awditi u eskalazzjoni tal-inċidenti.

3.5 Timmaniġġja bidliet fis-servizzi tal-forniturі u tiżgura proċedura ta' ħruġ sigura kif ukoll ir-ritorn jew it-tħassir tad-data mat-terminazzjoni.

3.6 Tallinja l-kontrolli tas-sigurtà ta' partijiet terzi mal-obbligi regolatorji u kuntrattwali applikabbli, inklużi l-GDPR, in-NIS2, id-DORA u l-istandards ISO/IEC 27001.

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-ISMS ġenerali, mal-ġestjoni tar-riskju u mal-istrateġija ta' konformità.

4.1.2 Japprova l-livelli ta' klassifikazzjoni tal-forniturі, l-eżiti tar-rieżamijiet tas-sigurtà u l-eċċezzjonijiet ta' riskju għoli.

4.1.3 Jipparteċipa fl-eskalazzjoni ta' inċidenti serji relatati mal-forniturі u fin-negozjati kuntrattwali għal servizzi kritiċi.

4.2 Akkwist u ġestjoni tal-forniturі

4.2.1 Jiżgura li l-kuntratti kollha ġodda u mġedda mal-forniturі jinkorporaw klawżoli approvati dwar is-sigurtà u l-protezzjoni tad-data.

4.2.2 Iżomm reġistru ċentralizzat tal-forniturі u jikkoordina mal-funzjonijiet Legali u ta' Konformità dwar id-dokumentazzjoni tar-riskju ta' partijiet terzi.

4.2.3 Jibda l-proċessi tal-onboarding u jiżgura l-allinjament mal-evalwazzjonijiet tas-sigurtà ta' qabel il-kuntratt.

[... 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-inqas darba fis-sena, jew qabel jekk iseħħ xi wieħed minn dawn li ġejjin:

9.1.1 Bidliet materjali fl-istrateġija tal-akkwist jew fl-ekosistema tal-forniturі

9.1.2 Aġġornamenti għall-oqfsa legali jew regolatorji (eż. DORA, GDPR)

9.1.3 Inċidenti kbar ta' partijiet terzi, ksur ta' data jew fallimenti tal-awditjar

9.1.4 Sejbiet minn evalwazzjonijiet tar-riskju jew minn korpi esterni ta' ċertifikazzjoni

9.2 Il-proċess tar-rieżami huwa ta’ sjieda konġunta bejn is-CISO, l-Akkwist, il-Legali u l-funzjonijiet tal-ġestjoni tar-riskju.

9.3 Ir-reviżjonijiet kollha tal-politika għandhom jiġu dokumentati fir-Reġistru tal-Kontroll tad-Dokumenti tal-ISMS, jinżammu taħt kontroll tal-verżjoni u jiġu kkomunikati lill-partijiet interessati rilevanti permezz tal-kanali ta’ governanza tal-forniturі u l-programmi ta’ sensibilizzazzjoni tal-impjegati.

9.4 Verżjonijiet sostitwiti għandhom jiġu arkivjati għal minimu ta’ tliet snin sabiex tiġi żgurata t-traċċabbiltà u l-konformità legali.

10. Politiki relatati u rabtiet

10.1 P1 – Politika tas-Sigurtà tal-Informazzjoni. Tistabbilixxi l-impenn ġenerali biex l-operazzjonijiet kollha tal-organizzazzjoni jinżammu siguri, inkluża d-dipendenza fuq forniturі ta’ partijiet terzi u forniturі esterni ta’ servizzi.

10.2 P6 – Politika tal-Ġestjoni tar-Riskju. Tiggwida l-identifikazzjoni, l-evalwazzjoni u l-mitigazzjoni tar-riskji assoċjati ma’ relazzjonijiet ma’ partijiet terzi, inklużi riskji inerenti jew sistemiċi mill-ekosistemi tal-forniturі.

10.3 P17 – Politika dwar il-Protezzjoni tad-Data u l-Privatezza. Tapplika għall-forniturі kollha li jimmaniġġjaw data personali, u tirrikjedi termini kuntrattwali xierqa, salvagwardji għat-trasferiment u prinċipji ta’ privatezza mid-disinn.

10.4 P4 – Politika dwar il-Kontroll tal-Aċċess. Tikkontrolla kif il-persunal ta’ partijiet terzi jikseb aċċess għas-sistemi tal-organizzazzjoni, billi timponi permessi bbażati fuq ir-rwoli, kontrolli tas-sessjonijiet u proċeduri ta’ revoka.

10.5 P22 – Politika tal-Illoggjar u l-Monitoraġġ. Tirrikjedi li l-aċċess tal-forniturі għas-sistemi jiġi mmonitorjat, illoggjat u rieżaminat, b’mod partikolari f’ambjenti fejn iseħħu attivitajiet privileġġjati jew iċċentrati fuq id-data.

10.6 P30 – Politika dwar ir-Rispons għall-Inċidenti. Tiddefinixxi l-proċeduri ta’ eskalazzjoni u r-rekwiżiti ta’ rappurtar ta’ ksur għal avvenimenti tas-sigurtà li joriġinaw mill-forniturі jew għal investigazzjonijiet konġunti li jinvolvu sistemi ta’ partijiet terzi.

11. Standards u oqfsa ta’ referenza

11.1 ISO/IEC 27001: Klawżola 8.1 – Ippjanar u Kontroll Operattiv: Tirrikjedi kontrolli formali fuq servizzi ta’ partijiet terzi li jaffettwaw l-ISMS.

11.2 ISO/IEC 27002:2022 – Kontrolli 5.19 sa 5.22:

11.2.1 Kontroll 5.19 tal-Anness A – Politiki u Proċeduri għar-Relazzjonijiet mal-Forniturі: Jirrikjedi kontrolli għall-ġestjoni tal-interazzjonijiet mal-forniturі.

11.2.2 Kontroll 5.20 tal-Anness A – Ġestjoni tar-Riskju tal-Forniturі: Jiffoka fuq l-identifikazzjoni, l-evalwazzjoni u s-sorveljanza kontinwa tal-pożizzjoni tas-sigurtà tal-fornitur.

11.2.3 Kontroll 5.21 tal-Anness A – Ġestjoni tat-Twassil tas-Servizzi tal-Forniturі: Jeħtieġ allinjament tal-prestazzjoni u tas-sigurtà mal-aspettattivi kuntrattwali.

11.2.4 Kontroll 5.22 tal-Anness A – Monitoraġġ u Rieżami tal-Forniturі: Isaħħaħ il-ħtieġa għal verifika u rivalutazzjoni kontinwa tal-konformità ta’ partijiet terzi.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SA-9 – Servizzi ta’ Sistemi Esterni: Jiddefinixxi rekwiżiti ta’ sigurtà u riskju għal sistemi operati minn entitajiet esterni.

11.3.2 SA-10 – Ġestjoni tal-Konfigurazzjoni mill-Iżviluppatur: Tapplika meta partijiet terzi jwasslu softwer jew ambjenti.

11.3.3 CA-3 – Interkonnessjonijiet tas-Sistemi: Tirrikjedi sorveljanza u qbil dwar il-flussi tad-data bejn l-entitajiet.

11.3.4 PS-7 – Sigurtà tal-Persunal ta’ Partijiet Terzi: Tiżgura li kuntratturi u persunal tal-fornitur ikunu skrinjati u mmonitorjati b’mod xieraq.

11.4 GDPR tal-UE (2016/679):

11.4.1 Artikolu 28 – Obbligi tal-proċessur: Jeħtieġ ftehimiet bil-miktub mal-proċessuri tad-data, inklużi miżuri tekniċi u organizzattivi (TOMs).

11.4.2 Artikolu 32 – Sigurtà tal-ipproċessar: Jobbliga salvagwardji xierqa kemm mill-kontrolluri kif ukoll mill-proċessuri.

11.4.3 Artikolu 33 – Notifika ta’ ksur ta’ data personali: Jeħtieġ notifika fil-pront mill-forniturі f’każ ta’ ksur.

11.5 Direttiva NIS2 tal-UE (2022/2555):

11.5.1 Artikolu 21(2)(e–f): Jeħtieġ ġestjoni tal-forniturі bbażata fuq ir-riskju u sorveljanza tas-sigurtà, b’mod partikolari fil-ktajjen tal-provvista diġitali ta’ entitajiet essenzjali u importanti.

11.6 DORA tal-UE (2022/2554):

11.6.1 Artikolu 28 – Riskju tal-ICT minn Partijiet Terzi: Jimponi obbligi għal evalwazzjoni tar-riskju, termini kuntrattwali tas-sigurtà u strateġiji ta’ ħruġ għal forniturі ta’ servizzi finanzjarji.

11.6.2 Artikolu 30 – Sorveljanza fuq Forniturі Kritiċi ta’ Partijiet Terzi tal-ICT: Jistabbilixxi aspettattivi msaħħa ta’ monitoraġġ u superviżjoni għal forniturі ewlenin.

11.7 COBIT 2019:

11.7.1 BAI05 – Ġestjoni tal-Abilitazzjoni tat-Tibdil Organizzattiv: Tiżgura li t-tranżizzjonijiet tal-forniturі jkunu rregolati b’mod sigur.

11.7.2 DSS02 – Ġestjoni tat-Talbiet għas-Servizz u l-Inċidenti: Tapplika għal kwistjonijiet irrappurtati mill-forniturі u għall-integrazzjoni tal-ġestjoni tal-inċidenti.

11.7.3 MEA03 – Monitoraġġ, Evalwazzjoni u Valutazzjoni tal-Konformità: Isaħħaħ il-kejl tal-prestazzjoni tal-fornitur u l-monitoraġġ tal-konformità.