					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P41					Titlu tad-dokument: **Politika tal-Ġestjoni tar-Riskju tad-Dipendenza fuq il-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	6.1.3, 8.1, 9.1	
ISO/IEC 27002:2022	5.20, 5.21, 5.22, 5.23, 5.30	
NIST SP 800-53 Rev.5	SR-2, SR-3, SR-5, SR-6, SR-11, RA-3	
GDPR tal-UE	Art. 28, Art. 32(1)(d)	
Direttiva NIS2 tal-UE	Art. 21(2)(d), Art. 21(3), Art. 22	
DORA tal-UE	Art. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Għan

1.1 Tissaħħaħ il-prattika tal-organizzazzjoni dwar is-sigurtà tal-katina tal-provvista billi jiġi stabbilit proċess għall-identifikazzjoni u l-ġestjoni ta' dipendenzi kritiċi fuq forniturі u forniturі tas-servizzi, kif meħtieġ mill-Artikolu 21(3) tan-NIS2 u mill-evalwazzjonijiet tar-riskju tal-katina tal-provvista fil-livell tal-Unjoni.

1.2 Jiġi żgurat li r-riskji li jirriżultaw minn konċentrazzjoni jew dipendenza fuq fornitur wieħed jinftiehmu u jiġu mitigati, u li kwalunkwe riskju tal-katina tal-provvista speċifiku għas-settur (kif enfasizzat mill-awtoritajiet skont l-Artikolu 22 tan-NIS2) jiġi inkorporat fil-Proċess tal-Ġestjoni tar-Riskju u fl-ippjanar tal-kontinwità tan-negozju tagħna.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għall-forniturі essenzjali kollha u għall-forniturі tas-servizzi li l-organizzazzjoni tiddependi fuqhom għal operazzjonijiet kritiċi, b'mod partikolari dawk fil-katina tal-provvista tal-ICT (hardware, software, cloud, telecom, servizzi ġestiti).

2.2 Tkopri funzjonijiet interni, inklużi l-Akkwist u d-diliġenza dovuta tal-forniturі, il-ġestjoni tal-forniturі, il-Proċess tal-Ġestjoni tar-Riskju, u d-dipartimenti operattivi rilevanti. Tinvolvi wkoll lill-forniturі nfushom sa fejn ikun meħtieġ għall-ġbir ta' informazzjoni dwar ir-riskju. "Forniturі kritiċi" huma dawk li n-nuqqas jew il-kompromess tagħhom jista' jħalli impatt sinifikanti fuq il-kapaċità tagħna li nwasslu servizzi jew inwettqu obbligi legali.

3. Objettivi

3.1 Tinkiseb viżibbiltà fuq id-dipendenzi fil-katina tal-provvista, b'mod partikolari billi jiġu identifikati punti uniċi ta' falliment jew riskju għoli ta' konċentrazzjoni fil-bażi tal-forniturі tagħna (eż. dipendenza fuq fornitur cloud wieħed għas-servizzi kollha).

3.2 Jiġu implimentati miżuri biex jitnaqqsu u jiġu ġestiti r-riskji relatati mal-forniturі, bħad-diversifikazzjoni, l-ippjanar ta' kontinġenza jew ir-rekwiżit għal kontrolli msaħħa min-naħa tal-fornitur, u b'hekk tissaħħaħ ir-reżiljenza kontra fallimenti tal-forniturі jew attakki li joriġinaw mill-katina tal-provvista.

3.3 Tiġi żgurata l-allinjament mar-rekwiżiti tan-NIS2 billi r-riżultati ta' kwalunkwe evalwazzjoni koordinata tar-riskji tas-sigurtà ta' ktajjen tal-provvista kritiċi (skont l-Artikolu 22) jiġu integrati fid-deċiżjonijiet organizzattivi dwar ir-riskju, u billi l-approċċ tagħna għar-riskju tal-katina tal-provvista jkun dokumentat u dimostrabbli.

4. Rwoli u responsabbiltajiet

4.1 Uffiċċju tal-Ġestjoni tal-Forniturі (VMO): huwa responsabbli għar-reġistru tad-dipendenzi fuq il-forniturі u jikkoordina l-evalwazzjonijiet tar-riskju. Jiżgura li, waqt l-onboarding inizjali u perjodikament wara dan, kull fornitur ewlieni jiġi evalwat għall-kritiċità u għal-livell ta' dipendenza.

4.2 Ġestjoni tar-Riskju (Kumitat tar-Riskju tal-Intrapriża): twettaq rieżami tar-riskju ta' konċentrazzjoni u tal-analiżijiet tad-dipendenza, tapprova l-istrateġiji tat-trattament tar-riskju (eż. approvazzjoni biex jiżdied fornitur alternattiv jew biex jinżamm inventarju addizzjonali għal komponenti kritiċi). Tinkorpora r-riskju tal-katina tal-provvista fir-Reġistru tar-Riskji ġenerali u tirrapporta lit-Tmexxija Għolja.

[... Is-sezzjonijiet 4.3–8 mhumiex inklużi f'dan il-preview. Ixtri d-dokument sħiħ biex taċċessa l-kontenut kollu. ...]

9. Monitoraġġ u awditjar

9.1 Ir-reġistru tad-dipendenzi u l-evalwazzjonijiet tar-riskju għandhom jiġu awditjati internament kull sena. L-Awditjar Intern għandu jivverifika li l-forniturі kritiċi kollha huma elenkati, li l-klassifikazzjonijiet tar-riskju tagħhom huma aġġornati, u li l-pjanijiet ta' mitigazzjoni huma fis-seħħ u qed javvanzaw. Għandu jiċċekkja wkoll li input minn evalwazzjonijiet esterni tar-riskju (rapporti tal-Artikolu 22, eċċ.) ikun ġie kkunsidrat kif dovut.

9.2 L-effettività tal-miżuri ta' diversifikazzjoni u ta' kontinġenza għandha tiġi ttestjata perjodikament. Pereżempju, tista' ssir simulazzjoni ppjanata fejn jiġi assunt li fornitur ewlieni jonqos, biex jiġu ttestjati l-pjanijiet ta' kontinwità u l-arranġamenti alternattivi tagħna (b'mod simili għal eżerċizzju ta' DR iżda għal qtugħ minn fornitur). Ir-riżultati ta' dawn it-testijiet għandhom jiġu dokumentati u kwalunkwe nuqqas għandu jiġi kkoreġut.

9.3 Metriċi: il-funzjoni tal-Ġestjoni tar-Riskju għandha ssegwi metriċi bħal "% tas-servizzi kritiċi li għandhom tal-anqas fornitur jew soluzzjoni alternattiva waħda disponibbli" jew "L-aqwa 5 dipendenzi fuq forniturі u x-xejra tar-riskju tagħhom". Dawn il-metriċi għandhom jiġu inklużi fid-daxxbords tar-riskju għat-tmexxija. It-tnaqqis fir-riskju tad-dipendenza maż-żmien huwa objettiv; jekk il-metriċi juru żieda fid-dipendenza, dan għandu jqajjem diskussjoni fil-livell tal-maniġment.

10. Rieżami u manutenzjoni

10.1 Din il-politika għandha tiġi rieżaminata tal-anqas kull sena mit-timijiet tal-ġestjoni tal-forniturі u tal-Ġestjoni tar-Riskju. Ir-rieżami għandu jinkorpora kwalunkwe bidla fil-pajsaġġ tal-forniturі (eż. jekk fornitur ġdid isir kritiku jew wieħed antik jitneħħa gradwalment) u kwalunkwe rekwiżit regolatorju ġdid dwar l-esternalizzazzjoni jew ir-riskju ta' partijiet terzi.

10.2 Jekk awtoritajiet settorjali joħorġu gwida aġġornata jew jekk inċident jiżvela lakuni (pereżempju, jekk qtugħ minn fornitur kellu impatt akbar milli kien antiċipat, u dan jindika li l-evalwazzjoni tar-riskju tagħna ma vvalutatx sew id-dipendenza), il-politika għandha tiġi aġġornata biex tirfina l-kriterji jew l-istrateġiji ta' mitigazzjoni.

10.3 Verżjonijiet riveduti tal-politika għandhom jiġu approvati mill-maniġment għoli. Bidliet sinifikanti għandhom jiġu kkomunikati lid-dipartimenti rilevanti kollha, u l-materjali tat-taħriġ għandhom jiġu aġġornati kif xieraq biex jirriflettu proċeduri jew standards ġodda.

11. Politiki relatati u rabtiet

11.1 P01 – Politika tas-Sigurtà tal-Informazzjoni. Tassenja r-responsabbiltà għall-governanza tad-dipendenza fuq il-forniturі.

11.2 P02 – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza. Tiċċara s-sjieda għad-deċiżjonijiet dwar ir-riskju tal-forniturі.

11.3 P06 – Politika tal-Ġestjoni tar-Riskju. Tinkorpora r-riskju ta' konċentrazzjoni fir-Reġistri tar-Riskji tal-intrapriża.

11.4 P26 – Politika tas-Sigurtà ta' Partijiet Terzi u tal-Forniturі. Linja bażi tas-sigurtà; P41 iżżid kontrolli dwar id-dipendenza/l-konċentrazzjoni.

11.5 P27 – Politika dwar l-Użu tal-Cloud. Tapplika kriterji ta' dipendenza għall-adozzjoni ta' servizzi cloud u għall-pjanijiet ta' ħruġ.

11.6 P28 – Politika dwar Żvilupp Esternalizzat. Tkopri riskji ta' dipendenza fl-inġinerija esterna.

11.7 P32 – Politika dwar il-Kontinwità tan-Negozju u l-Irkupru minn Diżastru. Tippjana għal xenarji ta' qtugħ jew sostituzzjoni ta' fornitur.

11.8 P37 – Politika dwar il-Konformità Legali u Regolatorja. Tiżgura li l-kuntratti u l-obbligi jirriflettu kontrolli tad-dipendenza.

12. Referenzi

12.1 Direttiva NIS2 (UE 2022/2555), Artikolu 21(3) (li jeħtieġ li jitqiesu vulnerabbiltajiet speċifiċi għal kull fornitur dirett/fornitur tas-servizzi u l-kwalità taċ-ċibersigurtà tagħhom, inklużi r-riżultati ta' evalwazzjonijiet koordinati tar-riskju tal-katina tal-provvista)

12.2 Direttiva NIS2, Artikolu 22(1) (evalwazzjonijiet koordinati tar-riskji tas-sigurtà ta' ktajjen tal-provvista kritiċi fil-livell tal-Unjoni – jinfurmaw lill-entitajiet dwar riskji settorjali relatati mal-forniturі)

12.3 Regolament ta' Implimentazzjoni tal-Kummissjoni (UE) 2024/2690, Taqsima 5 tal-Anness (rekwiżiti tas-sigurtà tal-katina tal-provvista għall-entitajiet, inklużi kriterji għall-għażla tal-forniturі, id-diversifikazzjoni u l-obbligi kuntrattwali)

12.4 Prattiki Tajbin tal-ENISA għaċ-Ċibersigurtà tal-Katina tal-Provvista (2022) – rakkomandazzjonijiet dwar l-identifikazzjoni ta' forniturі kritiċi u l-ġestjoni tar-riskji relatati

12.5 ISO/IEC 27001:2022 / ISO/IEC 27002:2022