					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P27					Titlu tad-dokument: **Politika dwar l-Użu tal-Cloud**							
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 mar-regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	Rekwiżiti għall-ippjanar u l-kontroll operattiv fil-cloud.
ISO/IEC 27002:2022	Kontrolli 5.23–5.25	Obbligi dwar l-użu, il-politika u s-sigurtà tas-servizzi cloud.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12 – SC-28, SR-5	Użu ta' sistemi esterni, rekwiżiti kuntrattwali u tekniċi, kontrolli kriptografiċi u protezzjoni tal-katina tal-provvista.
GDPR tal-UE	Artikoli 28, 32, Kapitolu V	Rekwiżiti għall-proċessuri cloud, is-sigurtà tal-ipproċessar u t-trasferimenti tad-data.
Direttiva NIS2 tal-UE	Artikolu 21(2)(f, i)	Rekwiżiti dwar ir-riskju ta' partijiet terzi u l-katina tal-provvista.
DORA tal-UE	Artikoli 5(2), 28	Sorveljanza tal-ICT u ta' partijiet terzi cloud għal entitajiet finanzjarji.
COBIT 2019	BAI04, DSS01, DSS05	Disponibbiltà tal-cloud, operazzjonijiet u ġestjoni tas-sigurtà.

1. Għan

1.1 Din il-politika tistabbilixxi r-rekwiżiti obbligatorji tal-organizzazzjoni għall-użu sigur, konformi u responsabbli tas-servizzi tal-cloud computing fil-mudelli ta' twassil Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) u Software-as-a-Service (SaaS).

1.2 Il-politika għandha l-għan li tiżgura li s-servizzi cloud jiġu adottati u ġestiti b'mod li jipproteġi l-Kunfidenzjalità, l-Integrità u d-Disponibbiltà (CIA) tal-assi tal-informazzjoni, filwaqt li jintlaħqu l-obbligi regolatorji, legali u kuntrattwali.

1.3 Hija tiddefinixxi kontrolli biex jiġi ġestit ir-riskju tal-cloud, tiġi protetta d-data, jiġi mmonitorjat il-livell ta' konformità tal-forniturі u jiġi eliminat l-użu mhux awtorizzat. Tappoġġa wkoll l-innovazzjoni fin-negozju permezz ta' pjattaformi cloud billi tallinja s-sigurtà, ir-reżiljenza operattiva u l-effiċjenza fl-ispejjeż.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għall-impjegati kollha, il-kuntratturi, il-forniturі ta' servizzi ta' partijiet terzi u l-konsulenti esterni li jipprovdu, jikkonfiguraw, jaċċessaw, jimmaniġġjaw jew jużaw servizzi cloud f'isem l-organizzazzjoni.

2.2 Hija tapplika għall-ambjenti kollha fejn tiġi pproċessata d-data jew il-workloads tal-organizzazzjoni, inklużi:

2.2.1 implimentazzjonijiet cloud pubbliċi, privati, ibridi u komunitarji

2.2.2 il-mudelli kollha ta' servizzi cloud (IaaS, PaaS, SaaS)

2.2.3 arkitetturi multi-cloud u federati

2.2.4 użu ta' shadow IT jew kontijiet cloud personali għal finijiet tan-negozju

2.3 Hija tkopri l-klassifikazzjonijiet kollha tad-data u tapplika kemm għal sistemi interni kif ukoll għal pjattaformi ospitati mill-fornituri fejn tinħażen jew tiġi pproċessata data li hija proprjetà tal-organizzazzjoni jew data rregolata.

3. Objettivi

3.1 Jiġi żgurat użu sigur u konsistenti tat-teknoloġiji cloud permezz ta' linji gwida ddefiniti b'mod ċar, linji bażi tas-sigurtà u rwoli ta' governanza.

3.2 Jiġu minimizzati r-riskji operattivi u regolatorji marbuta mal-cloud computing, inklużi aċċess mhux awtorizzat, ksur tad-data, konfigurazzjoni ħażina, nuqqas ta' konformità u tfixkil fis-servizz.

3.3 Jiġu applikati rekwiżiti ta' sigurtà u privatezza għall-fornituri cloud kollha u tiġi vverifikata l-konformità permezz ta' klawżoli kuntrattwali, evalwazzjonijiet u drittijiet ta' awditjar.

3.4 Tiġi permessa adozzjoni tal-cloud skalabbli u reżiljenti mingħajr kompromess fil-pożizzjoni tas-sigurtà, fir-rekwiżiti legali jew fil-kontinwità tan-negozju.

3.5 Il-governanza u l-użu tal-cloud jiġu allinjati mal-qafas tal-ISMS tal-organizzazzjoni, mal-obbligi legali (eż. GDPR, DORA), mal-linji gwida speċifiċi għas-settur u mal-aħjar prattiki rikonoxxuti fl-industrija (eż. NIST, COBIT).

4. Rwoli u responsabbiltajiet

4.1 Maniġment Eżekuttiv

4.1.1 Japprova l-Politika dwar l-Użu tal-Cloud u l-pjan direzzjonali strateġiku għall-adozzjoni tal-cloud.

4.1.2 Jirrieżamina u japprova eċċezzjonijiet ta' riskju għoli għar-rekwiżiti standard ta' governanza tal-cloud.

4.1.3 Jiżgura li l-inizjattivi cloud jirċievu finanzjament adegwat, sorveljanza u integrazzjoni mal-oqfsa tar-riskju tal-intrapriża.

4.2 Uffiċjal Ewlieni tas-Sigurtà tal-Informazzjoni (CISO)

4.2.1 Huwa s-sid ta' din il-politika u tar-Reġistru tas-Servizzi Cloud tal-organizzazzjoni.

4.2.2 Japprova l-onboarding ta' fornituri cloud ġodda abbażi tad-diliġenza dovuta u tal-valutazzjoni tar-riskju.

4.2.3 Jirrieżamina d-dokumentazzjoni tal-konformità tal-fornitur u jivverifika l-allinjament mar-rekwiżiti tas-sigurtà.

[... 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 u aġġornata kif meħtieġ biex jinżamm allinjament kontinwu ma':

9.1.1 rekwiżiti legali u regolatorji li qed jevolvu (eż. GDPR, NIS2, DORA)

9.1.2 bidliet fl-istandards ISO/IEC 27001 jew ISO/IEC 27002

9.1.3 aġġornamenti fl-arkitettura cloud, fil-pajsaġġ tat-theddid jew fil-portafoll tas-servizzi tal-organizzazzjoni

9.1.4 investigazzjonijiet ta' inċidenti, riżultati tal-awditjar jew tagħlimiet miksuba mill-użu operattiv

9.2 Il-CISO huwa responsabbli biex jibda r-rieżami u jiġbor il-partijiet interessati rilevanti, inklużi:

9.2.1 il-Perit tas-Sigurtà tal-Cloud

9.2.2 it-Tim Legali u ta' Konformità

9.2.3 il-Maniġers tal-Akkwist u tal-Fornituri

9.2.4 is-Sidien tas-Servizz u Operazzjonijiet tal-IT

9.3 L-aġġornamenti kollha għandhom ikunu:

9.3.1 taħt kontroll tal-verżjoni u ddatati

9.3.2 approvati mill-Maniġment Eżekuttiv

9.3.3 ikkomunikati lill-partijiet affettwati, inklużi impjegati, kuntratturi u partijiet terzi

9.3.4 arkivjati skont il-politiki interni tad-dokumentazzjoni

9.4 Rieżamijiet interim jistgħu jiġu attivati minn:

9.4.1 impenji ġodda ma' CSPs jew migrazzjonijiet ewlenin

9.4.2 theddid emerġenti għall-infrastruttura cloud

9.4.3 bidliet materjali f'obbligi kuntrattwali, legali jew speċifiċi għas-settur

10. Politiki relatati u rabtiet

10.1 Din il-politika hija marbuta mill-qrib ma' u tiddependi fuq il-politiki interni li ġejjin:

10.1.1 P1 – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi l-prinċipji ġenerali li jirregolaw l-operat sigur tas-sistemi u s-servizzi, li din il-politika tapplika fil-kuntest tal-cloud.

10.1.2 P5 – Politika tal-Ġestjoni tat-Tibdil: Il-bidliet kollha fil-konfigurazzjoni tal-cloud għandhom isegwu l-proċeduri ta' kontroll tat-tibdil deskritti fil-P5.

10.1.3 P13 – Politika ta' Klassifikazzjoni u Tikkettar tad-Data: Tiddetermina kif id-data tiġi evalwata qabel it-trasferiment lejn il-cloud u kif jiġu applikati kontrolli bħall-iċċifrar u r-residenza tad-data.

10.1.4 P18 – Politika tal-Kontrolli Kriptografiċi: Tipprovdi standards għall-iċċifrar, il-ġestjoni taċ-ċwievet u l-użu ta' algoritmi kriptografiċi, applikati direttament fil-konfigurazzjonijiet tas-servizzi cloud.

10.1.5 P22 – Politika tal-Logging u l-Monitoraġġ: Tispeċifika rekwiżiti għall-ġbir, iż-żamma u l-analiżi tal-logs li għandhom jiġu applikati f'ambjenti cloud.

10.1.6 P30 – Politika dwar ir-Rispons għall-Inċidenti: Tiddefinixxi l-proċeduri ta' eskalazzjoni, trażżin u rimedjazzjoni għal avvenimenti ta' sigurtà relatati mal-cloud.

10.1.7 P33 – Politika tal-Monitoraġġ tal-Awditjar u l-Konformità: Tappoġġa l-kapaċità li tintwera l-konformità u l-assigurazzjoni kontinwa li l-kontrolli tal-cloud huma applikati u mmonitorjati.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001: Klawżola 8.1 – Ippjanar u Kontroll Operattiv: Teħtieġ li l-organizzazzjonijiet jimplimentaw u jikkontrollaw il-proċessi meħtieġa biex jintlaħqu r-rekwiżiti tas-sigurtà tal-informazzjoni, inklużi dawk li jinvolvu ambjenti cloud.

11.2 ISO/IEC 27002:2022 – Kontrolli 5.23 sa 5.25:

11.2.1 Anness A Kontroll 5.23 – Użu tas-Servizzi Cloud: Jeħtieġ valutazzjoni bbażata fuq ir-riskju, awtorizzazzjoni formali u dokumentazzjoni tal-użu tas-servizzi cloud.

11.2.2 Anness A Kontroll 5.24 – Politika dwar l-Użu tal-Cloud: Jeħtieġ l-istabbiliment u l-applikazzjoni ta' politiki formali dwar l-użu tal-cloud allinjati mal-ħtiġijiet u r-riskji tal-organizzazzjoni.

11.2.3 Anness A Kontroll 5.25 – Sigurtà fis-Servizzi Cloud: Jeħtieġ integrazzjoni tas-sigurtà, protezzjonijiet kuntrattwali u monitoraġġ ta' workloads u data ospitati fil-cloud.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – Użu ta' Sistemi Esterni: Jeħtieġ regoli u kundizzjonijiet definiti għall-aċċess għar-riżorsi tal-organizzazzjoni minn sistemi esterni jew f'ambjent cloud.

11.3.2 SA-9(5) – Servizzi ta' Sistemi ta' Informazzjoni Esterni: Jeħtieġ rekwiżiti kuntrattwali ta' sigurtà, sorveljanza u monitoraġġ kontinwu għal sistemi cloud ta' partijiet terzi.

11.3.3 SC-12 sa SC-28 – Protezzjonijiet Kriptografiċi, Protezzjoni tal-Konfini u Integrità tat-Trasmissjoni: Huma allinjati mar-rekwiżiti ta' iċċifrar, identità u aċċess għal servizzi ospitati fil-cloud u data fi tranżitu.

11.3.4 SR-5 – Protezzjoni tal-Katina tal-Provvista: Tappoġġa l-verifika u l-kontroll kuntrattwali fuq CSPs involuti fit-twassil tas-servizz.

11.4 GDPR tal-UE (2016/679):

11.4.1 Artikolu 28 – Obbligi tal-Proċessur: Jeħtieġ kuntratti formali mal-forniturі cloud biex tiġi żgurata s-sigurtà, il-kunfidenzjalità u l-awditabbiltà tal-ipproċessar tad-data personali.

11.4.2 Artikolu 32 – Sigurtà tal-Ipproċessar: Jappoġġa l-applikazzjoni tal-iċċifrar, kontrolli tal-aċċess, logging u salvagwardji oħra f'ambjenti cloud.

11.4.3 Kapitolu V – Trasferimenti Internazzjonali tad-Data: Jeħtieġ it-trasferiment legali ta' data barra l-UE/ŻEE billi jintużaw salvagwardji bħall-SCCs jew deċiżjonijiet ta' adegwatezza.

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

11.5.1 Artikolu 21(2)(f, i): Jeħtieġ li l-entitajiet jimmaniġġjaw ir-riskji minn forniturі cloud ta' partijiet terzi u jiżguraw l-integrità tal-katina tal-provvista diġitali permezz ta' miżuri kuntrattwali u tekniċi.

11.6 DORA tal-UE (2022/2554):

11.6.1 Artikolu 5(2) – Governanza tar-Riskji tal-ICT: Jeħtieġ l-integrazzjoni tar-riskju tal-ICT ta' partijiet terzi, inklużi s-servizzi cloud, fil-governanza ġenerali tar-riskju.

11.6.2 Artikolu 28 – Sorveljanza ta' Forniturі Kritiċi Terzi tal-ICT: Jeħtieġ li l-entitajiet finanzjarji jimmonitorjaw, jikkontrollaw u jirrappurtaw dwar id-dipendenzi fuq forniturі cloud, il-pożizzjoni tas-sigurtà u r-reżiljenza tagħhom.

11.7 COBIT 2019:

11.7.1 BAI04 – Ġestjoni tad-Disponibbiltà u l-Kapaċità: Jiżgura li s-servizzi cloud ikunu reżiljenti, monitorjati u jissodisfaw kriterji ta' prestazzjoni definiti.

11.7.2 DSS01 – Ġestjoni tal-Operazzjonijiet: Jappoġġa l-integrazzjoni operattiva, il-ġestjoni tal-inċidenti u l-konfigurazzjonijiet bażi fil-pjattaformi ospitati fil-cloud.

11.7.3 DSS05 – Ġestjoni tas-Servizzi tas-Sigurtà: Jagħti direzzjoni għall-implimentazzjoni ta' kontrolli tas-sigurtà speċifiċi għall-cloud, monitoraġġ u prevenzjoni ta' inċidenti fis-servizzi diġitali.