

				Dañhal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P27S				Titlu tad-dokument: <b>Politika dwar l-Użu tas-Servizzi tal-Cloud</b>							
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	Ivvedut minn	Sid tal-proċess

Approvazzjonijiet			
Isem	Pożizzjoni	Data	Firma

**Avviż legali (drittijiet tal-awtur u restrizzjonijiet fuq l-użu)**  
(C) 2025 Clarysec LLC. All rights reserved.

Dan id-dokument huwa proprjetà intellettuali ta' Clarysec LLC. L-ebda parti minn dan id-dokument ma tista' tiġi kkupjata, użata mill-ġdid, distribwita jew modifikata għal skopijiet kummerċjali jew ta' implimentazzjoni mingħajr awtorizzazzjoni espliċita minn qabel bil-miktub.

L-użu mhux awtorizzat huwa strettament ipprojbit u jista' jwassal għal azzjoni legali.

Għal-liċenzjar, ikkuntattja: [info@clarysec.com](mailto:info@clarysec.com)

## Allinjata ma' standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	
ISO/IEC 27002:2022	Kontrolli 5.23–5.25	
NIST SP 800-53 Rev.5	AC-20, SC-12, SC-13, SR-5	
GDPR tal-UE	Artikolu 28, 32, u Kapitolu V	
Direttiva NIS2 tal-UE	Artikoli 21(2)(f), (i)	
DORA tal-UE	Artikoli 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI04	

### 1. Għan

1.1 Din il-politika tiddefinixxi kif is-servizzi tal-cloud jistgħu jintużaw b'mod sigur fi ħdan l-organizzazzjoni. Hija tiżgura li d-data pproċessata jew maħżuna fil-cloud tkun protetta, li l-aċċess ikun ikkontrollat, u li r-riskji jiġu ġestiti b'mod responsabbli.

1.2 Hija tgħin lill-SMEs jissodisfaw l-obbligi legali u l-aspettattivi tal-klijenti għall-protezzjoni ta' informazzjoni sensitiva, il-prevenzjoni ta' tnixxijiet ta' data, u l-ġestjoni effettiva tar-riskji f'ambjent cloud mingħajr il-ħtieġa ta' infrastruttura fuq skala ta' intrapriża.

1.3 Din il-politika tappoġġa ċ-ċertifikazzjoni ISO/IEC 27001, il-konformità mal-GDPR, u l-assigurazzjoni tal-katina tal-provvista permezz ta' governanza konsistenti tas-servizzi kollha tal-cloud ta' partijiet terzi.

### 2. Kamp ta' applikazzjoni

#### 2.1 Din il-politika tapplika għal:

2.1.1 Kull servizz cloud użat biex jaħžen, jipproċessa jew jittrasmetti data tal-kumpanija

2.1.2 Il-personal kollu, il-kuntratturi, u l-fornituri tas-servizzi li jużaw għodod cloud f'isem l-organizzazzjoni

2.1.3 Soluzzjonijiet cloud bla ħlas u bi ħlas, inklużi pjattaformi tal-imejl, qsim ta' dokumenti, għodod SaaS, pjattaformi tal-backup, video conferencing, u pjattaformi tal-klijenti

2.1.4 Kull apparat (desktop, mobile, tablet) li jaċċessa informazzjoni tal-kumpanija permezz ta' applikazzjonijiet cloud

#### 2.2 Dan jinkludi, iżda mhux limitat għal:

2.2.1 Microsoft 365, Google Workspace, Dropbox Business

2.2.2 Zoom, Microsoft Teams, Google Meet

2.2.3 AWS, Azure, GCP

2.2.4 Għodod cloud għall-backup u għall-irkupru mid-diżastri

2.2.5 Folders kondiviżi jew applikazzjonijiet użati għall-fatturazzjoni, il-ġestjoni tal-proġetti, jew il-komunikazzjoni mal-klijenti

### 3. Obiettivi

3.1 Tipprevjeni l-użu mhux awtorizzat jew ta' riskju għoli ta' servizzi cloud mhux approvati.

3.2 Tiżgura li data sensitiva jew data regolata maħżuna fil-cloud tkun protetta permezz ta' salvagwardji tekniċi u amministrattivi xierqa.

3.3 Tiddefinixxi rwoli ċari għall-approvazzjoni, il-konfigurazzjoni, il-monitoraġġ, u d-dekummissjonar tas-servizzi cloud.

3.4 Tikkontrolla l-flussi tad-data u tiżgura l-konformità mal-obbligi taż-żamma, it-tfassir, u l-privatezza għall-informazzjoni maħżuna fil-cloud.

3.5 Tnaqqas id-dipendenza fuq kontijiet personali jew għodod mhux traċċati billi tirrikjedi approvazzjoni għas-sistemi cloud kollha użati għal skopijiet tan-negożju.

3.6 Tiżgura konformità mar-rekwiżiti ta' ISO/IEC 27001:2022, il-GDPR, NIS2, u DORA għall-ġestjoni tad-dipendenzi esterni tal-cloud.

#### **4. Rwoli u responsabbiltajiet**

##### **4.1 Maniġer Ġenerali (GM)**

4.1.1 Japprova l-użu tas-servizzi cloud ġodda kollha

4.1.2 Jirrevedi r-riskji relatati mal-fornituri cloud u mat-tipi ta' servizzi

4.1.3 Jiżgura l-konformità ma' din il-politika u jissorvelja d-deċiżjonijiet dwar l-eċċezzjonijiet

##### **4.2 Fornitur ta' Appoġġ tal-IT jew Appoġġ Tekniku**

4.2.1 Jevalwa u jimplementa konfigurazzjoni sigura għas-servizzi cloud

4.2.2 Jistabilixxi kontijiet, kontrolli tal-aċċess, u soluzzjonijiet tal-backup

4.2.3 Jimmonitorja l-konformità mar-rekwiżiti tal-passwords, tal-awtentikazzjoni b'diversi fatturi, u tal-issettjar tas-sigurtà

[ ... Is-sezzjonijiet 4.3–8 mhumiex inkluzi 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 riveduta mill-inqas darba fis-sena mill-Maniġer Ġenerali, f'koordinazzjoni mal-Fornitur ta' Appoġġ tal-IT.

##### **9.2 Għandu jsir ukoll rieżami formali:**

9.2.1 Wara incident tas-sigurtà relatat mal-cloud (eż. ksur, telf ta' data)

9.2.2 Meta tiġi introdotta pjattaforma cloud ewlenija ġdida

9.2.3 Jekk jinbidlu r-rekwiżiti legali jew regolatorji (eż. aġġornamenti tal-GDPR, NIS2, DORA)

9.2.4 Jekk l-attivitajiet ta' monitoraġġ jiżvelaw użu ħażin jew riskji ġodda

##### **9.3 Il-GM għandu jiżgura:**

9.3.1 Li r-Registru tas-Servizzi Cloud jiġi aġġornat b'servizzi ġodda jew irtirati

9.3.2 Li r-rekwiżiti legali u tal-privatezza għandhom qed jiġu ssodisfati

9.3.3 Li l-bidliet kollha jiġu kkomunikati lill-utenti u lill-partijiet interessati rilevanti

9.4 Verżjonijiet arkivjati għandhom jinħażnu b'mod sigur, u verżjonijiet qodma tal-politika għandhom jiġu ġestiti skont il-P14S – Politika ta' żamma u rimi tad-data tal-organizzazzjoni.

#### **10. Politiki relatati u rabtiet**

##### **10.1 Din il-politika għandha tintuża f'koordinazzjoni mal-politiki li ġejjin ta' sigurtà tal-informazzjoni allinjati għall-SME:**

10.1.1 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tiddefinixxi r-responsabbiltà għall-approvazzjoni tas-servizzi cloud u għall-ġestjoni tar-relazzjonijiet mal-fornituri.

10.1.2 P4S – Politika dwar il-Kontroll tal-Aċċess: Tappoġġa prattiki siguri ta' login, ġestjoni tas-sessjonijiet, u revoka meħtieġa għall-pjattaformi cloud.

10.1.3 P14S – Politika ta' żamma u rimi tad-data: Tirregola kif data f'ambjent cloud tiġi appoġġata b'backup, tinzamm, u titfassar skont l-obbligi legali.

10.1.4 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tiżgura li kwalunkwe data personali maħżuna fis-servizzi cloud tiġi ġestita skont il-prinċipji tal-GDPR.

10.1.5 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tipprovdi proċeduri strutturati għar-rispons għal inċidenti ta' sigurtà relatati mal-cloud, inklużi l-ġbir tal-evidenza u n-notifika esterna.

10.2 Flimkien, dawn il-politiki jiżguraw li l-użu tal-cloud ikun sigur, konformi, u reżiljenti mil-lat operattiv.

## **11. Standards u oqfsa ta' referenza**

### **11.1 ISO/IEC 27001**

11.1.1 Klawżola 8.1 – Teħtieġ li l-organizzazzjonijiet jimplimentaw kontrolli operattivi għall-ġestjoni tad-data, inklużi dawk relatati ma' sistemi cloud.

### **11.2 ISO/IEC 27002**

11.2.1 Kontroll 5.23 – Jeħtieġ governanza fuq l-użu tas-servizzi cloud u l-għodod SaaS minn partijiet terzi.

11.2.2 Kontroll 5.24 – Jeħtieġ politika definita dwar l-użu tal-cloud allinjata mar-riskju u mar-rekwiżiti regolatorji.

11.2.3 Kontroll 5.25 – Jeħtieġ li l-organizzazzjonijiet jiżguraw li l-kontrolli tas-sigurtà f'ambjenti cloud jissodisfaw il-ħtiġijiet tal-organizzazzjoni.

### **11.3 NIST SP 800-53 Rev.5**

11.3.1 AC-20 – Jeħtieġ politiki formali ta' użu għal sistemi esterni bħas-servizzi cloud.

11.3.2 SC-12, SC-13 – Jindirizzaw l-iċċifrar għal data fi tranżitu u data maħżuna f'ambjenti cloud.

11.3.3 SR-5 – Ikopri kontrolli tar-riskju tal-cloud u ta' partijiet terzi fil-katina tal-provvista.

### **11.4 GDPR tal-UE (2016/679)**

11.4.1 Artikolu 28 – Jeħtieġ li fornituri cloud li jaġixxu bħala proċessuri tad-data jsegwu obbligi kuntrattwali vinkolanti.

11.4.2 Artikolu 32 – Jobbliga kontrolli tekniċi u organizzattivi għall-ipproċessar tad-data f'ambjent cloud.

11.4.3 Kapitolu V – Jipprojbixxi trasferimenti internazzjonali mhux awtorizzati ta' data personali maħżuna fil-cloud.

### **11.5 Direttiva NIS2 tal-UE (2022/2555)**

11.5.1 Artikolu 21(2)(f), (i) – Jeħtieġ li entitajiet essenzjali u importanti jimplimentaw politiki xierqa għas-sigurtà tas-servizzi cloud u għall-kontroll tal-katina tal-provvista.

### **11.6 DORA tal-UE (2022/2554)**

11.6.1 Artikolu 5(2) – Jeħtieġ li SMEs finanzjarji jintegraw is-sigurtà tal-cloud fil-qafas tagħhom ta' ġestjoni tar-riskju tal-ICT.

11.6.2 Artikolu 28 – Jistabbilixxi regoli ta' sorveljanza għall-fornituri kritiċi terzi ta' servizzi tal-ICT, inklużi fornituri cloud.

### **11.7 COBIT 2019**

11.7.1 DSS01 – “Manage Operations” jindirizza l-integrità operattiva tas-servizzi cloud.

11.7.2 DSS05 – “Manage Security Services” jinkludi protezzjonijiet u monitoraġġ speċifiċi għall-cloud.

11.7.3 BAI04 – “Manage Availability and Capacity” jiżgura l-kontinwità tan-negozju u l-prestazzjoni f'ambjenti cloud.