					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P27S					Titolo del documento: **Politica sull'utilizzo dei servizi cloud**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineata a standard e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	
ISO/IEC 27002:2022	Controlli 5.23–5.25	
NIST SP 800-53 Rev.5	AC-20, SC-12, SC-13, SR-5	
GDPR UE	Articolo 28, 32 e Capitolo V	
NIS2 UE	Articoli 21(2)(f), (i)	
DORA UE	Articoli 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI04	

1. Finalità

1.1 La presente politica definisce le modalità con cui i servizi cloud possono essere utilizzati in modo sicuro all'interno dell'organizzazione. Garantisce che i dati trattati o archiviati nel cloud siano protetti, che gli accessi siano controllati e che i rischi siano gestiti in modo appropriato.

1.2 Essa supporta le piccole e medie imprese (PMI) nel soddisfare gli obblighi normativi e le aspettative dei clienti in materia di protezione delle informazioni sensibili, prevenzione della perdita di dati e gestione efficace dei rischi connessi al cloud, senza richiedere infrastrutture di livello enterprise.

1.3 La presente politica supporta la certificazione ISO/IEC 27001, la conformità al GDPR e la sicurezza della supply chain attraverso una governance coerente di tutti i servizi cloud di terze parti.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 Qualsiasi servizio cloud utilizzato per archiviare, trattare o trasmettere dati aziendali

2.1.2 Tutto il personale, i collaboratori esterni e i fornitori di servizi che utilizzano strumenti cloud per conto dell'organizzazione

2.1.3 Soluzioni cloud gratuite e a pagamento, incluse piattaforme di posta elettronica, condivisione documentale, strumenti SaaS, piattaforme di backup, videoconferenza e portali clienti

2.1.4 Qualsiasi dispositivo (desktop, mobile, tablet) che acceda a informazioni aziendali tramite applicazioni cloud

2.2 Ciò include, a titolo esemplificativo e non esaustivo:

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 Strumenti cloud per il backup e il disaster recovery

2.2.5 Cartelle condivise o applicazioni utilizzate per la fatturazione, la gestione dei progetti o la comunicazione con i clienti

3. Obiettivi

3.1 Prevenire l'uso non autorizzato o ad alto rischio di servizi cloud non approvati.

3.2 Garantire che i dati sensibili o soggetti a requisiti normativi archiviati nel cloud siano protetti mediante controlli tecnici e organizzativi appropriati.

3.3 Definire ruoli chiari per l'approvazione, la configurazione, il monitoraggio e la dismissione dei servizi cloud.

3.4 Controllare i flussi di dati e applicare gli obblighi di conservazione, cancellazione e tutela della privacy relativi alle informazioni archiviate nel cloud.

3.5 Ridurre il ricorso ad account personali o strumenti non tracciati richiedendo l'approvazione di tutti i sistemi cloud utilizzati per finalità aziendali.

3.6 Soddisfare i requisiti di ISO/IEC 27001:2022, GDPR, NIS2 e DORA per la gestione delle dipendenze esterne da servizi cloud.

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 Approva l'utilizzo di tutti i nuovi servizi cloud

4.1.2 Riesamina i rischi relativi ai fornitori cloud e alle tipologie di servizio

4.1.3 Assicura l'applicazione della presente politica e supervisiona le decisioni in materia di eccezioni

4.2 Fornitore IT o referente tecnico

4.2.1 Valuta e implementa la configurazione sicura dei servizi cloud

4.2.2 Configura account, controlli di accesso e backup

4.2.3 Monitora la conformità delle impostazioni relative a password, autenticazione a più fattori (MFA) e sicurezza

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Requisiti di riesame e aggiornamento

9.1 La presente politica deve essere riesaminata almeno annualmente dal Direttore generale, in coordinamento con il fornitore IT.

9.2 Un riesame formale deve inoltre essere effettuato:

9.2.1 A seguito di un incidente di sicurezza connesso al cloud (ad esempio violazione o perdita di dati)

9.2.2 Quando viene introdotta una nuova piattaforma cloud rilevante

9.2.3 In caso di modifica dei requisiti legali o normativi (ad esempio aggiornamenti di GDPR, NIS2, DORA)

9.2.4 Se le attività di monitoraggio rilevano usi impropri o nuovi rischi

9.3 Il Direttore generale deve garantire che:

9.3.1 Il Registro dei servizi cloud sia aggiornato con i nuovi servizi o con quelli dismessi

9.3.2 I requisiti legali e in materia di privacy continuino a essere soddisfatti

9.3.3 Tutte le modifiche siano comunicate agli utenti e alle parti interessate pertinenti

9.4 Le versioni archiviate devono essere conservate in modo sicuro e le versioni precedenti della politica devono essere gestite in conformità alla P14S – Politica di conservazione e smaltimento dei dati dell'organizzazione.

10. Politiche correlate e collegamenti

10.1 La presente politica deve essere applicata congiuntamente alle seguenti politiche di sicurezza delle informazioni allineate alle PMI:

10.1.1 P2S – Politica sui ruoli e le responsabilità di governance: definisce le responsabilità per l'approvazione dei servizi cloud e la gestione dei rapporti con i fornitori.

10.1.2 P4S – Politica di controllo degli accessi: supporta pratiche sicure di accesso, gestione delle sessioni e revoca degli accessi richieste per le piattaforme cloud.

10.1.3 P14S – Politica di conservazione e smaltimento dei dati: disciplina le modalità di backup, conservazione e cancellazione dei dati archiviati nel cloud in conformità agli obblighi di legge.

10.1.4 P17S – Politica di protezione dei dati e privacy: garantisce che tutti i dati personali archiviati nei servizi cloud siano trattati secondo i principi del GDPR.

10.1.5 P30S – Politica di risposta agli incidenti (P30): fornisce procedure strutturate per la risposta agli incidenti di sicurezza cloud, inclusa la raccolta delle evidenze e la notifica esterna.

10.2 Nel loro insieme, queste politiche garantiscono che l'utilizzo del cloud sia sicuro, conforme e resiliente dal punto di vista operativo.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1 – Richiede alle organizzazioni di implementare controlli operativi per il trattamento dei dati, compresi quelli relativi ai sistemi basati sul cloud.

11.2 ISO/IEC 27002

11.2.1 Controllo 5.23 – Richiede la governance dell'utilizzo dei servizi cloud e degli strumenti SaaS di terze parti.

11.2.2 Controllo 5.24 – Richiede una politica definita sull'uso del cloud allineata ai requisiti di rischio e normativi.

11.2.3 Controllo 5.25 – Richiede alle organizzazioni di garantire che i controlli di sicurezza negli ambienti cloud soddisfino le esigenze organizzative.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-20 – Richiede politiche d'uso formali per sistemi esterni quali i servizi cloud.

11.3.2 SC-12, SC-13 – Riguardano la cifratura dei dati in transito e dei dati a riposo negli ambienti cloud.

11.3.3 SR-5 – Copre i controlli sul rischio cloud e di terze parti nella supply chain.

11.4 GDPR UE (2016/679)

11.4.1 Articolo 28 – Richiede che i fornitori cloud che agiscono come responsabili del trattamento rispettino obblighi contrattuali vincolanti.

11.4.2 Articolo 32 – Richiede misure tecniche e organizzative per il trattamento dei dati basato sul cloud.

11.4.3 Capitolo V – Vieta trasferimenti internazionali non autorizzati di dati personali archiviati nel cloud.

11.5 Direttiva UE NIS2 (2022/2555)

11.5.1 Articolo 21(2)(f), (i) – Richiede ai soggetti essenziali e importanti di implementare politiche adeguate per la sicurezza dei servizi cloud e il controllo della supply chain.

11.6 Regolamento UE DORA (2022/2554)

11.6.1 Articolo 5(2) – Richiede alle PMI finanziarie di integrare la sicurezza del cloud nei propri quadri di riferimento per la gestione del rischio ICT.

11.6.2 Articolo 28 – Stabilisce regole di vigilanza per i fornitori terzi critici di servizi ICT, inclusi i fornitori cloud.

11.7 COBIT 2019

11.7.1 DSS01 – "Manage Operations" riguarda l'integrità operativa dei servizi cloud.

11.7.2 DSS05 – "Manage Security Services" include misure di protezione e monitoraggio specifiche per il cloud.

11.7.3 BAI04 – "Manage Availability and Capacity" garantisce continuità operativa e prestazioni negli ambienti cloud.