					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P27					Titolo del documento: **Politica di utilizzo del 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 norme e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	Requisiti di pianificazione operativa e controllo per gli ambienti cloud.
ISO/IEC 27002:2022	Controlli 5.23–5.25	Prescrizioni relative all'uso, alla politica e alla sicurezza dei servizi cloud.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12–SC-28, SR-5	Uso di sistemi esterni, requisiti contrattuali e tecnici, protezioni crittografiche, protezione della catena di fornitura.
GDPR UE	Articoli 28, 32, Capitolo V	Requisiti per i responsabili del trattamento cloud, sicurezza del trattamento, trasferimenti dei dati.
NIS2 UE	Articolo 21(2)(f, i)	Requisiti relativi al rischio delle terze parti e alla catena di fornitura.
DORA UE	Articoli 5(2), 28	Vigilanza sui sistemi ICT e sulle terze parti (cloud) per le entità finanziarie.
COBIT 2019	BAI04, DSS01, DSS05	Disponibilità del cloud, operazioni, gestione della sicurezza.

1. Finalità

1.1 La presente politica stabilisce i requisiti obbligatori dell'organizzazione per l'uso sicuro, conforme e responsabile dei servizi di cloud computing nei modelli di erogazione Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) e Software-as-a-Service (SaaS).

1.2 La politica ha l'obiettivo di garantire che i servizi cloud siano adottati e governati in modo da proteggere la riservatezza, l'integrità e la disponibilità (CIA) degli asset informativi, nel rispetto degli obblighi normativi, legali e contrattuali.

1.3 Definisce i controlli per gestire il rischio cloud, proteggere i dati, monitorare la conformità dei fornitori ed eliminare gli utilizzi non autorizzati. Supporta inoltre l'innovazione aziendale attraverso piattaforme cloud, allineando sicurezza, affidabilità operativa ed efficienza dei costi.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i dipendenti, collaboratori esterni, fornitori di servizi terzi e consulenti esterni che effettuano il provisioning, configurano, accedono, gestiscono o utilizzano servizi cloud per conto dell'organizzazione.

2.2 Si applica a tutti gli ambienti in cui sono trattati dati o carichi di lavoro dell'organizzazione, inclusi:

2.2.1 Cloud pubblici e privati, ambienti ibridi e community cloud

2.2.2 Tutti i modelli di servizio cloud (IaaS, PaaS, SaaS)

2.2.3 Architetture multi-cloud e federate

2.2.4 Utilizzo di shadow IT o di account cloud personali per finalità aziendali

2.3 Copre tutti i livelli di classificazione dei dati e si applica sia ai sistemi interni sia alle piattaforme ospitate dai fornitori nelle quali sono archiviati o trattati dati di proprietà dell'organizzazione o soggetti a regolamentazione.

3. Obiettivi

3.1 Garantire un utilizzo sicuro e coerente delle tecnologie cloud mediante linee guida chiaramente definite, baseline di sicurezza e ruoli di governance.

3.2 Ridurre al minimo i rischi operativi e normativi associati al cloud computing, inclusi accessi non autorizzati, violazioni dei dati, configurazioni errate, non conformità e interruzioni del servizio.

3.3 Assicurare l'applicazione dei requisiti di sicurezza e privacy a tutti i fornitori cloud e verificarne la conformità attraverso clausole contrattuali, valutazioni e clausole di diritto di audit.

3.4 Consentire un'adozione del cloud scalabile e resiliente senza compromettere il livello di sicurezza, i requisiti legali o la continuità operativa.

3.5 Allineare la governance e l'utilizzo del cloud con il framework SGSI dell'organizzazione, gli obblighi legali (ad es. GDPR, DORA), le linee guida settoriali e le migliori pratiche riconosciute (ad es. NIST, COBIT).

4. Ruoli e responsabilità

4.1 Direzione aziendale

4.1.1 Approva la Politica di utilizzo del cloud e la roadmap strategica per l'adozione del cloud.

4.1.2 Riesamina e approva le eccezioni ad alto rischio ai requisiti standard di governance del cloud.

4.1.3 Garantisce che le iniziative cloud dispongano di finanziamenti adeguati, supervisione e integrazione con i framework aziendali di gestione del rischio.

4.2 Responsabile della sicurezza delle informazioni (CISO)

4.2.1 È il titolare della politica e del registro organizzativo dei servizi cloud.

4.2.2 Approva l'onboarding di nuovi fornitori cloud sulla base della due diligence sui fornitori e della valutazione del rischio.

4.2.3 Riesamina la documentazione di conformità del fornitore e ne convalida l'allineamento ai requisiti di 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 e aggiornata secondo necessità per garantire il continuo allineamento con:

9.1.1 L'evoluzione dei requisiti legali e normativi (ad es. GDPR, NIS2, DORA)

9.1.2 Le modifiche alle norme ISO/IEC 27001 o ISO/IEC 27002

9.1.3 Gli aggiornamenti all'architettura cloud dell'organizzazione, al panorama dei rischi o al portafoglio dei servizi

9.1.4 Le indagini sugli incidenti, i risultati degli audit o le lezioni apprese dall'utilizzo operativo

9.2 Il CISO è responsabile dell'avvio del riesame e della convocazione delle parti interessate pertinenti, tra cui:

9.2.1 Architetto della sicurezza cloud

9.2.2 Funzione Legale e Compliance

9.2.3 Responsabili Acquisti e fornitori

9.2.4 Proprietari dei servizi e Operations IT

9.3 Tutti gli aggiornamenti devono essere:

9.3.1 Soggetti a controllo di versione e datati

9.3.2 Approvati dalla Direzione aziendale

9.3.3 Comunicati alle parti interessate coinvolte, inclusi dipendenti, collaboratori esterni e terze parti

9.3.4 Archiviati in conformità alle politiche interne di gestione documentale

9.4 Riesami intermedi possono essere attivati da:

9.4.1 Nuovi rapporti con CSP o migrazioni di sistema rilevanti

9.4.2 Rischi emergenti per l'infrastruttura cloud

9.4.3 Modifiche significative agli obblighi contrattuali, legali o settoriali

10. Politiche correlate e collegamenti

10.1 La presente politica è strettamente collegata alle seguenti politiche interne e dipende da esse:

10.1.1 P1 – Politica per la sicurezza delle informazioni: stabilisce i principi generali che disciplinano il funzionamento sicuro di sistemi e servizi, che la presente politica applica nel contesto cloud.

10.1.2 P5 – Politica di gestione delle modifiche: tutte le modifiche alla configurazione cloud devono seguire le procedure di controllo delle modifiche descritte nella P5.

10.1.3 P13 – Politica di classificazione ed etichettatura dei dati: determina come i dati sono valutati prima del trasferimento nel cloud e come vengono applicati controlli quali cifratura e localizzazione dei dati.

10.1.4 P18 – Politica sui controlli crittografici: definisce le regole per la cifratura, la gestione delle chiavi e l'utilizzo degli algoritmi crittografici, applicate direttamente nelle configurazioni dei servizi cloud.

10.1.5 P22 – Politica di registrazione e monitoraggio: specifica i requisiti per la raccolta, la conservazione e l'analisi dei log, che devono essere applicati negli ambienti cloud.

10.1.6 P30 – Politica di risposta agli incidenti (P30): definisce le procedure di escalation, contenimento e rimedio per gli eventi di sicurezza correlati al cloud.

10.1.7 P33 – Politica di monitoraggio dell'audit e della conformità: supporta la capacità di dimostrare la conformità in sede di audit e la garanzia continua che i controlli cloud siano applicati e monitorati.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001: Clausola 8.1 – Pianificazione operativa e controllo: richiede alle organizzazioni di attuare e controllare i processi necessari a soddisfare i requisiti di sicurezza delle informazioni, compresi quelli che coinvolgono ambienti cloud.

11.2 ISO/IEC 27002:2022 – Controlli da 5.23 a 5.25:

11.2.1 Allegato A, Controllo 5.23 – Uso dei servizi cloud: prescrive una valutazione basata sul rischio, un'autorizzazione formale e la documentazione dell'utilizzo dei servizi cloud.

11.2.2 Allegato A, Controllo 5.24 – Politica di utilizzo del cloud: richiede la definizione e l'applicazione di politiche formali sull'utilizzo del cloud allineate alle esigenze e ai rischi dell'organizzazione.

11.2.3 Allegato A, Controllo 5.25 – Sicurezza nei servizi cloud: impone l'integrazione della sicurezza, le protezioni contrattuali e il monitoraggio dei carichi di lavoro e dei dati ospitati nel cloud.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – Uso di sistemi esterni: richiede regole e condizioni definite per accedere alle risorse dell'organizzazione da sistemi esterni o basati su cloud.

11.3.2 SA-9(5) – Servizi di sistemi informativi esterni: impone requisiti contrattuali di sicurezza, vigilanza e monitoraggio continuo per i sistemi cloud di terze parti.

11.3.3 SC-12 a SC-28 – Protezioni crittografiche, difesa del perimetro e integrità della trasmissione: sono allineati ai requisiti di cifratura, identità e accesso per i servizi ospitati nel cloud e per i dati in transito.

11.3.4 SR-5 – Protezione della catena di fornitura: supporta la valutazione e il controllo contrattuale dei CSP coinvolti nell'erogazione dei servizi.

11.4 GDPR UE (2016/679):

11.4.1 Articolo 28 – Obblighi del responsabile del trattamento: richiede contratti formali con i fornitori cloud per garantire sicurezza, riservatezza e verificabilità del trattamento dei dati personali.

11.4.2 Articolo 32 – Sicurezza del trattamento: supporta l'applicazione di cifratura, controlli degli accessi, registrazione e altre misure di sicurezza negli ambienti cloud.

11.4.3 Capitolo V – Trasferimenti internazionali di dati: impone il trasferimento lecito dei dati al di fuori dell'UE/SEE mediante misure di salvaguardia quali SCC o decisioni di adeguatezza.

11.5 Direttiva UE NIS2 (2022/2555):

11.5.1 Articolo 21(2)(f, i): richiede alle entità di gestire i rischi derivanti dai fornitori terzi di servizi cloud e di garantire l'integrità della catena di fornitura digitale attraverso misure contrattuali e tecniche.

11.6 DORA UE (2022/2554):

11.6.1 Articolo 5(2) – Governance dei rischi ICT: prescrive l'integrazione del rischio ICT di terze parti, inclusi i servizi cloud, nella governance complessiva del rischio.

11.6.2 Articolo 28 – Vigilanza sui fornitori terzi critici di servizi ICT: richiede alle entità finanziarie di monitorare, controllare e rendicontare le dipendenze dai fornitori cloud, il livello di sicurezza e la resilienza.

11.7 COBIT 2019:

11.7.1 BAI04 – Gestire disponibilità e capacità: garantisce che i servizi cloud siano resilienti, monitorati e soddisfino i criteri di prestazione definiti.

11.7.2 DSS01 – Gestire le operazioni: supporta l'integrazione operativa, la gestione degli incidenti e le configurazioni baseline nelle piattaforme ospitate nel cloud.

11.7.3 DSS05 – Gestire i servizi di sicurezza: indirizza l'attuazione di controlli di sicurezza specifici per il cloud, il monitoraggio e la prevenzione degli incidenti nei servizi digitali.