POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

SGSI Anthesi S.r.l. - servizi SaaS e cloud

Codice	POL-SGSI-01	**Revisione**	0
Data emissione	12/08/2026	**Classificazione**	PUBBLICO
Redazione	Responsabile SGSI	**Approvazione**	Direzione
Riferimento	ISO/IEC 27001:2022 § 5.2	**Integrazioni**	ISO/IEC 27017 e ISO/IEC 27018

Dichiarazione della Direzione

Anthesi S.r.l., nello svolgimento delle attività di progettazione, sviluppo, erogazione, manutenzione e supporto di servizi digitali, SaaS e cloud, riconosce le informazioni, i dati dei clienti, i dati personali, il software, le configurazioni, le credenziali e il know-how come asset essenziali per la continuità e l'affidabilità dei servizi. La Direzione assume la sicurezza delle informazioni come principio di governo aziendale e come requisito da integrare nei processi, nelle decisioni tecnologiche, nei rapporti con clienti e fornitori e nella gestione del personale.

1. Finalità e quadro di riferimento

La presente Politica definisce i principi e gli impegni dell'Alta Direzione per il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI). Essa costituisce il quadro di riferimento per la definizione e il riesame degli obiettivi di sicurezza e si applica al campo di applicazione formalmente definito nel DOC-SGSI-4.3.

Il SGSI è sviluppato con riferimento alla ISO/IEC 27001:2022 e relativo Amendment 1:2024. Per i servizi cloud sono considerate le linee guida ISO/IEC 27017 nell'edizione vigente applicabile; per la protezione dei dati personali nei servizi di public cloud, quando Anthesi opera come PII processor per conto del cliente, sono considerate le linee guida ISO/IEC 27018:2025. I requisiti cogenti, regolamentari, contrattuali e specifici dei clienti sono recepiti nel SGSI quando applicabili.

2. Principi della sicurezza delle informazioni

Anthesi orienta il proprio SGSI ai seguenti principi:

- Riservatezza: accesso alle informazioni esclusivamente da parte di soggetti, processi e servizi autorizzati.
- Integrità: protezione dell'accuratezza, completezza e affidabilità delle informazioni e delle configurazioni contro modifiche non autorizzate o accidentali.
- Disponibilità: accessibilità delle informazioni e dei servizi agli utenti autorizzati secondo le esigenze operative e gli impegni concordati.
- Autenticità e tracciabilità: capacità di attribuire in modo affidabile identità, operazioni ed eventi rilevanti.
- Approccio basato sul rischio: priorità e misure di sicurezza sono determinate sulla base dei rischi, dei requisiti applicabili e del valore degli asset.
- Responsabilità condivisa nel cloud: i confini di responsabilità tra Anthesi, clienti e provider devono essere identificati, documentati e governati.
- Protezione dei PII: i dati personali sono trattati secondo il ruolo privacy effettivamente assunto da Anthesi e secondo le istruzioni, i contratti e le norme applicabili.

3. Impegni dell'Alta Direzione

La Direzione si impegna a:

- assicurare che la Politica sia appropriata alle finalità, al contesto, ai servizi e ai rischi di Anthesi e sia coerente con gli indirizzi strategici;

- definire obiettivi di sicurezza misurabili o verificabili, coerenti con la presente Politica, e valutarne periodicamente il conseguimento;
- soddisfare i requisiti legali, regolamentari, contrattuali e gli altri requisiti applicabili alla sicurezza delle informazioni e alla protezione dei dati;
- identificare, valutare, trattare e riesaminare i rischi per la sicurezza delle informazioni, approvando i criteri e le decisioni di accettazione del rischio residuo;
- mettere a disposizione risorse, competenze, tecnologie e responsabilità adeguate al funzionamento e al miglioramento del SGSI;
- integrare la sicurezza delle informazioni nei processi di progettazione, sviluppo, modifica, rilascio, erogazione e supporto dei servizi SaaS e cloud;
- prevenire, rilevare, registrare e gestire eventi, vulnerabilità e incidenti di sicurezza, assicurando comunicazioni tempestive secondo ruoli e requisiti applicabili;
- proteggere le informazioni lungo il relativo ciclo di vita, inclusi creazione, acquisizione, utilizzo, condivisione, conservazione, backup, trasferimento, restituzione e cancellazione;
- governare gli accessi secondo i principi di necessità, minimo privilegio, separazione dei compiti, autenticazione adeguata e riesame periodico;
- qualificare e monitorare i fornitori e i cloud provider rilevanti, considerando dipendenze, SLA, sicurezza, resilienza, subfornitura e capacità di uscita/migrazione;
- promuovere competenza, consapevolezza e responsabilizzazione del personale e dei collaboratori, richiedendo la segnalazione degli eventi di sicurezza;
- monitorare le prestazioni del SGSI, svolgere audit interni e riesami di Direzione e attuare azioni correttive quando necessarie;
- migliorare continuamente l'idoneità, l'adeguatezza e l'efficacia del SGSI.

4. Impegni specifici per i servizi cloud

Nell'erogazione e nell'utilizzo di servizi cloud, Anthesi si impegna inoltre a:

- definire e mantenere chiare le responsabilità di sicurezza nei rapporti in cui Anthesi opera come Cloud Service Provider (CSP) verso i clienti e come Cloud Service Customer (CSC) verso i propri provider;
- governare configurazioni, identità, privilegi, interfacce, logging, monitoraggio e segregazione logica in funzione dei rischi e delle responsabilità effettivamente assegnate;
- valutare la sicurezza dei provider cloud e le relative dipendenze, senza trasferire al fornitore le responsabilità che rimangono in capo ad Anthesi;
- considerare, ove pertinenti, portabilità, recuperabilità, restituzione e cancellazione sicura dei dati e i rischi di lock-in nella gestione dell'intero ciclo di vita del servizio;
- mantenere sotto controllo i cambiamenti del servizio cloud che possono modificare il profilo di rischio o gli impegni assunti verso i clienti.

5. Impegni specifici per la protezione dei PII

Quando, nell'ambito di servizi di public cloud, Anthesi tratta PII per conto di un cliente in qualità di responsabile/PII processor, la Direzione assicura che il trattamento sia governato in modo coerente con le istruzioni documentate, gli accordi applicabili e le responsabilità privacy effettivamente assunte.

- limitare il trattamento dei PII alle finalità, istruzioni, tempi e soggetti autorizzati applicabili;
- proteggere i PII con misure tecniche e organizzative proporzionate al rischio;
- governare sub-responsabili e terze parti che trattano PII, assicurando obblighi di sicurezza e protezione dei dati coerenti con quelli assunti da Anthesi;
- supportare il cliente/titolare, per quanto di competenza, nella gestione di incidenti, richieste degli interessati e obblighi previsti dagli accordi e dalla normativa;
- assicurare processi controllati per restituzione, trasferimento e cancellazione dei PII alla cessazione del servizio o quando richiesto e applicabile;
- preservare trasparenza, tracciabilità e disponibilità delle evidenze necessarie a dimostrare il rispetto degli impegni assunti.

6. Quadro di riferimento per gli obiettivi

Gli obiettivi di sicurezza sono stabiliti e riesaminati considerando almeno: risultati del Risk Assessment e del Piano di Trattamento, requisiti dei clienti e SLA, incidenti ed eventi, vulnerabilità, prestazioni dei servizi e dei fornitori, esiti di audit e riesami, cambiamenti tecnologici e organizzativi, requisiti normativi e contrattuali e opportunità di miglioramento. Gli obiettivi sono assegnati a responsabili identificati e, quando possibile, associati a indicatori, target, scadenze e criteri di verifica.

7. Comunicazione, disponibilità e riesame

La Politica è mantenuta come informazione documentata, comunicata all'interno dell'organizzazione e resa disponibile alle parti interessate rilevanti con modalità appropriate. Il personale e i collaboratori sono tenuti a conoscerne i principi e ad applicare le regole di sicurezza pertinenti al proprio ruolo. La sua diffusione deve essere supportata da evidenze verificabili.

La Direzione riesamina la Politica almeno in occasione del Riesame di Direzione e comunque quando intervengano cambiamenti significativi nel contesto, nel campo di applicazione, nei servizi cloud, nei requisiti applicabili, nei rischi, negli asset o a seguito di incidenti rilevanti che ne rendano opportuna la revisione.

8. Approvazione

Approvato da	Direzione
Data	12/08/2026
Firma / approvazione documentale	_____