Sommario

1 Premessa 2
2 Impegni per la qualità 2
3 Impegni per la sicurezza delle informazioni 2
4 Servizi Cloud 3
5 Protezione dei dati personali 3
6 Intelligenza artificiale 4
7 Persone, cultura e condotta etica 4
8 Obiettivi e miglioramento continuo 4
9 Applicabilità e responsabilità 4
10 Comunicazione e riesame 5

Rev.	Data	Motivo modifica	Firma Approvazione Direzione
0	15/05/2025	Prima emissione (Politica sicurezza delle informazioni)	
1	09/07/2026	Politica integrata qualità e sicurezza delle informazioni: ISO 9001, estensioni ISO/IEC 27017 e 27018, protezione dei dati personali, intelligenza artificiale	DEEPCUBE Srl Via Gran Sasso, 1 66100 CHIETI P.IVA e C.F. 02629920691

1 Premessa

DEEPCUBE S.r.l. sviluppa software, applicazioni web e mobile, servizi SaaS e soluzioni basate sull'intelligenza artificiale per imprese di medie e grandi dimensioni. Valutati il contesto in cui opera e le esigenze delle parti interessate, la Direzione ha istituito e mantiene un Sistema di Gestione Integrato (SGI) conforme alle norme ISO 9001:2015 e ISO/IEC 27001:2022, esteso ai controlli delle ISO/IEC 27017 per i servizi cloud e ISO/IEC 27018 per la protezione dei dati personali nel cloud pubblico.
La Direzione attribuisce importanza strategica alla qualità dei prodotti e servizi e alla protezione del patrimonio informativo, proprio e dei clienti, e si impegna a sviluppare, attuare, controllare e migliorare in modo costante il SGI. La presente politica si applica al campo di applicazione del SGI: ideazione, progettazione, sviluppo e fornitura di software client/server destinato ad applicazioni web e dispositivi mobili, con utilizzo di algoritmi di intelligenza artificiale.

2 Impegni per la qualità

La Direzione si impegna a:

- **soddisfare i requisiti dei clienti,** quelli cogenti e quelli sottoscritti volontariamente;
- **mettere il cliente al centro**, comprendendone le esigenze, anche implicite, rispettando tempi e impegni concordati e misurandone la soddisfazione;
- **lavorare per processi controllati**, dalla raccolta dei requisiti al supporto post-rilascio, con riesami, verifiche e validazioni pianificate e tracciabili;
- **decidere sulla base delle evidenze**: indicatori, dati di test, informazioni di ritorno dei clienti, esiti degli audit;
- **selezionare e tenere sotto controllo i fornitori esterni**, inclusi servizi cloud, sviluppatori esterni, componenti open source e servizi di intelligenza artificiale di terze parti.

3 Impegni per la sicurezza delle informazioni

Gli obiettivi principali del SGI per la sicurezza delle informazioni sono assicurare:

- **riservatezza**: l'informazione non è resa disponibile né comunicata a individui, entità o processi non autorizzati;
- **integrità**: sono tutelate l'accuratezza e la completezza delle informazioni e degli asset;
- **disponibilità**: l'informazione è accessibile e utilizzabile su richiesta di un'entità autorizzata;
- **conformità** ai requisiti cogenti, normativi e contrattuali di sicurezza.

Per questo la Direzione si impegna a:

- adottare una metodologia di valutazione del rischio adeguata e gestire il rischio a un livello accettabile, in coerenza con la gestione del rischio strategico;
- proteggere le informazioni da accessi non autorizzati in funzione della loro classificazione, valore e sensibilità, secondo la Politica di classificazione delle informazioni (POL-SI-20);
- mantenere un'architettura di sicurezza fondata su regole, strumenti e controlli coerenti, inclusa la riduzione della superficie di attacco dei sistemi (PG-SI-06);
- garantire la continuità operativa dei processi e dei servizi erogati ai clienti;
- garantire ai clienti canali efficaci per lo scambio di informazioni e per il supporto in ogni evento che possa pregiudicare la sicurezza delle informazioni.

4 Servizi Cloud

DeepCube opera come cliente di servizi cloud (piattaforma Google Workspace) e come fornitore di servizi SaaS ai propri clienti. Nel rispetto della ISO/IEC 27017 e della Politica integrativa per la sicurezza delle informazioni in ambito Cloud (POL-SI-21), la Direzione si impegna a:

- definire e documentare la ripartizione delle responsabilità di sicurezza con il fornitore cloud e con i clienti;
- assicurare la segregazione degli ambienti dei clienti e degli ambienti di sviluppo e produzione;
- gestire in modo sicuro l'accesso amministrativo, il monitoraggio dei servizi e la comunicazione degli incidenti ai clienti;
- garantire la restituzione e la cancellazione sicura dei dati dei clienti al termine del servizio;
- selezionare fornitori cloud che offrano garanzie adeguate e verificarle nel tempo.

5 Protezione dei dati personali

Il trattamento dei dati personali avviene nel rispetto del Reg. UE 2016/679 (GDPR), del D.Lgs. 196/2003 e della Politica di protezione dei dati personali (POL-SI-18), applicando i principi di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, privacy by design e by default. Quando tratta dati personali per conto dei clienti nei servizi cloud, DeepCube agisce come responsabile del trattamento e, secondo la ISO/IEC 27018, si impegna a:

- trattare i dati solo secondo le istruzioni documentate del cliente titolare e mai per finalità proprie, comprese quelle di marketing o pubblicità;
- rendere trasparenti l'uso di sub-responsabili e i luoghi di trattamento dei dati;
- assistere i clienti nelle richieste di esercizio dei diritti degli interessati;
- notificare tempestivamente ai clienti le violazioni di dati personali;
- vincolare alla riservatezza tutto il personale che accede ai dati personali.

È nominato un Responsabile della protezione dei dati (DPO), punto di riferimento per ogni questione legata alla protezione dei dati personali.

6 Intelligenza artificiale

Lo sviluppo, la fornitura e l'utilizzo di sistemi di intelligenza artificiale avvengono in modo responsabile, trasparente e conforme al Reg. UE 2024/1689 (AI Act), secondo la Politica per l'Intelligenza Artificiale (POL-AI-01).

7 Persone, cultura e condotta etica

La Direzione assicura persone competenti, con formazione continua su qualità, sicurezza delle informazioni, protezione dei dati e intelligenza artificiale, e ruoli e responsabilità chiari. Promuove una cultura in cui la qualità e la sicurezza sono responsabilità di tutti e i comportamenti sono improntati a integrità, trasparenza e rispetto, secondo il Codice Etico. Chi rileva un errore, un difetto, un punto debole o un incidente lo segnala subito al Responsabile del SGI, senza timore di conseguenze: le segnalazioni servono a capire le cause e a migliorare.

8 Obiettivi e miglioramento continuo

La presente politica costituisce il quadro di riferimento per fissare gli obiettivi per la qualità e per la sicurezza delle informazioni, definiti annualmente dalla Direzione nel Piano di miglioramento e obiettivi con indicatori, traguardi, responsabili e scadenze. Gli obiettivi riguardano almeno: affidabilità del software, rispetto degli impegni, assistenza, soddisfazione del cliente, competenze, efficacia dei controlli di sicurezza e continuità dei servizi. La Direzione rende disponibili le risorse necessarie e si impegna a migliorare in modo continuo il SGI e i suoi risultati.

9 Applicabilità e responsabilità

La politica si applica a tutto il personale e ai collaboratori di DeepCube e ai fornitori che operano nel campo di applicazione del SGI. È formulata e riesaminata dalla Direzione; il Responsabile del SGI ne facilita l'attuazione tramite politiche, procedure e istruzioni appropriate. Tutto il personale e i collaboratori sono tenuti a rispettare la politica e le

regole che la attuano. Qualsiasi azione che, intenzionalmente o per negligenza, arrechi danno a DeepCube, ai suoi clienti o agli interessati potrà essere perseguita nelle sedi opportune.

10 Comunicazione e riesame

La politica è comunicata al personale e ai collaboratori al momento dell'inserimento e durante la formazione periodica, è disponibile nel repository documentale aziendale ed è resa disponibile alle parti interessate anche tramite il sito web. È riesaminata almeno annualmente, in occasione del Riesame della Direzione, e ogni volta che cambiano il contesto, la strategia o i requisiti applicabili, per assicurarne la continua idoneità.