Information Security Management System

Doc. **PO-ISMS.001** Ed. **1** - Rev. **0** del **09/01/2025**
Classificazione: **C1 PUBBLICO**

Politica aziendale per la Sicurezza delle Informazioni

Ai Engineering s.r.l.
Sede Legale e operativa
C.so Francesco Ferrucci, 112 - 10138 Torino (TO)
P.IVA IT 06764910011
C.F/ Registro imprese TO 01066850064
Cod. REA: TO – 632269

1 SCHEDA DEL DOCUMENTO

Elenco delle modifiche:

Ed.	Rev.	REDAZIONE	LISTA CAMBIAMNETI	VERIFICA E APPROVAZIONE	
				ENTITA'	DATA
1	0	ISM	Prima Redazione all'interno del ISMS	CEO	09/01/2025

2 ELENCO DEI CONTENUTI

1 SCHEDA DEL DOCUMENTO 2
2 ELENCO DEI CONTENUTI 3
3 PREMESSA 4
4 SCOPO 4
5 CONTESTO DELL'ORGANIZZAZIONE 4
6 PARTI INTERESSATE E LORO REQUISITI 4
7 DEFINIZIONE DI SICUREZZA DELLE INFORMAZIONI 4
8 AMBITO DI APPLICAZIONE 4
9 OBIETTIVI 4
10 STRATEGIE OPERATIVE 5
11 PRINCIPI GUIDA 5
12 IMPEGNO DELLA DIREZIONE 5
13 RUOLI, RESPONSABILITÀ E AUTORITÀ 5
14 ECCEZIONI 5
15 VIOLAZIONI E SANZIONI 5
16 SEGNALAZIONE DELLE VIOLAZIONI 6
17 VALIDITÀ, REVISIONE E APPROVAZIONE 6
18 RIFERIMENTI NORMATIVI E DOCUMENTALI 6

3 PREMESSA

Ai Engineering S.r.l. (di seguito "Ai Engineering" o "organizzazione") svolge attività integrata di consulenza e servizi altamente specializzati nell'ingegneria civile, rivolgendosi a una clientela composta da enti pubblici e soggetti privati. Le competenze maturate dall'organizzazione si estendono ai settori dell'edilizia, dell'ambiente, delle infrastrutture e dei trasporti, con un approccio multidisciplinare e orientato all'innovazione.

In un contesto in cui la digitalizzazione assume un ruolo sempre più centrale nei processi produttivi e gestionali, e dove le minacce informatiche si fanno più sofisticate, Ai Engineering riconosce la protezione delle informazioni aziendali come una componente strategica della propria attività. La sicurezza delle informazioni è pertanto considerata un elemento essenziale per tutelare la competitività, garantire la continuità operativa e rafforzare la fiducia di clienti, partner e stakeholder.

4 SCOPO

La presente Politica per la Sicurezza delle Informazioni ha lo scopo di definire in modo chiaro e strutturato l'approccio dell'organizzazione alla protezione del proprio patrimonio informativo. L'obiettivo è quello di prevenire accessi non autorizzati, perdite, manipolazioni, distruzioni o indisponibilità delle informazioni gestite. In tal modo si intende assicurare non solo la tutela dei dati aziendali, ma anche la salvaguardia degli interessi dei soggetti con cui l'organizzazione intrattiene relazioni professionali e istituzionali.

5 CONTESTO DELL'ORGANIZZAZIONE

Ai Engineering opera in un mercato altamente competitivo e dinamico, dove le trasformazioni tecnologiche e normative impongono una continua evoluzione delle modalità operative. L'organizzazione, parte del più ampio Gruppo Ai, affronta quotidianamente sfide legate alla gestione di dati sensibili, alla digitalizzazione dei processi e all'utilizzo di infrastrutture tecnologiche avanzate, inclusi ambienti cloud e soluzioni di collaborazione distribuita. Il contesto normativo in cui si inserisce comprende regolamenti europei e nazionali, standard tecnici internazionali e requisiti contrattuali derivanti da progetti complessi. Tale scenario impone una costante attenzione alla sicurezza delle informazioni, che deve essere considerata non solo come un obbligo di conformità, ma anche come un valore organizzativo.

6 PARTI INTERESSATE E LORO REQUISITI

L'organizzazione riconosce che la sicurezza delle informazioni è influenzata dalle esigenze e dalle aspettative di una pluralità di soggetti con cui interagisce. I clienti richiedono affidabilità nella gestione dei dati e garanzie di riservatezza. I dipendenti e i collaboratori si attendono di operare in un ambiente dove le informazioni siano protette e i rischi ridotti al minimo. Anche fornitori e consulenti devono poter contare su regole chiare che disciplinino l'accesso e il trattamento dei dati aziendali. Le autorità di controllo, infine, richiedono il rispetto puntuale delle normative vigenti e l'adozione di sistemi di gestione conformi agli standard riconosciuti. Ai Engineering si impegna a tenere conto di tutte queste esigenze, integrandole nel proprio sistema di gestione e adattando le proprie misure di sicurezza alle aspettative legittime delle parti interessate.

7 DEFINIZIONE DI SICUREZZA DELLE INFORMAZIONI

Per Ai Engineering, la sicurezza delle informazioni rappresenta l'insieme delle misure, dei controlli e delle pratiche organizzative volte a proteggere le informazioni da eventi che ne possano compromettere la riservatezza, l'integrità e la disponibilità. La riservatezza consiste nel garantire che l'accesso alle informazioni sia limitato esclusivamente a chi è autorizzato. L'integrità assicura che le informazioni siano accurate, complete e protette da modifiche non autorizzate, sia intenzionali che accidentali. La disponibilità implica che le informazioni e i sistemi che le gestiscono siano accessibili e fruibili da parte dei soggetti legittimati, nel momento in cui ne hanno bisogno.

8 AMBITO DI APPLICAZIONE

La presente Politica si applica a tutte le informazioni trattate da Ai Engineering, indipendentemente dalla loro forma (digitale, cartacea, orale), dalla loro natura (tecnica, commerciale, amministrativa, personale) o dalla loro classificazione. Essa riguarda tutte le persone che accedono, trattano, trasmettono o gestiscono informazioni per conto dell'organizzazione, inclusi dipendenti, collaboratori, fornitori e consulenti esterni formalmente autorizzati. Rientrano nell'ambito di applicazione anche i sistemi informativi, le infrastrutture tecnologiche, i dispositivi, le sedi fisiche e digitali (inclusi ambienti cloud e sedi remote) coinvolti nel trattamento delle informazioni.

9 OBIETTIVI

La politica si propone di garantire la resilienza dei sistemi informativi aziendali, la tutela del know-how e della proprietà intellettuale, la riduzione dell'impatto di eventuali incidenti informatici e la conformità ai requisiti legali, contrattuali e normativi di settore. Essa mira anche a promuovere la consapevolezza del personale riguardo alla sicurezza delle informazioni e a rendere visibile l'impegno dell'organizzazione nei confronti dei propri stakeholder. Gli obiettivi di sicurezza vengono tradotti annualmente in risultati misurabili, formalizzati all'interno del Piano Annuale della Sicurezza e monitorati attraverso indicatori di performance (KPI) specifici. Tali indicatori sono oggetto di verifica nel corso del Riesame della Direzione e servono come base per eventuali azioni correttive e migliorative.

10 STRATEGIE OPERATIVE

Per realizzare gli obiettivi delineati, Ai Engineering ha adottato un Information Security Management System (ISMS) conforme alla norma ISO/IEC 27001:2022. L'organizzazione si impegna a condurre valutazioni periodiche dei rischi, a implementare controlli basati sulla classificazione delle informazioni, a monitorare gli eventi di sicurezza e a garantire una risposta tempestiva e strutturata agli incidenti. Particolare attenzione viene riservata alla formazione del personale, alla sensibilizzazione sui comportamenti sicuri e all'esecuzione di audit interni mirati a verificare l'efficacia del sistema. Tali strategie sono supportate da un approccio sistematico al miglioramento continuo, che si concretizza attraverso l'analisi dei risultati, l'apprendimento derivante dagli incidenti, l'adeguamento dei controlli e il costante aggiornamento della documentazione.

11 PRINCIPI GUIDA

La sicurezza delle informazioni presso Ai Engineering si fonda su alcuni principi fondamentali. Le informazioni vengono classificate in base alla loro sensibilità, valore e criticità, al fine di determinare il livello adeguato di protezione. L'accesso alle informazioni è regolato dal principio del "need-to-know", garantendo che solo il personale debitamente autorizzato possa accedere ai dati necessari per lo svolgimento delle proprie funzioni. L'utilizzo della crittografia è obbligatorio per la protezione delle informazioni più sensibili, sia in fase di memorizzazione che durante la trasmissione. Sono inoltre adottate misure per assicurare l'integrità e la disponibilità dei dati, comprese soluzioni di backup, infrastrutture ridondate e procedure di manutenzione preventiva. La conservazione delle informazioni avviene in conformità ai requisiti normativi e contrattuali, mentre la loro eliminazione segue modalità sicure e documentate. Tutte le misure adottate sono proporzionate al livello di rischio identificato.

12 IMPEGNO DELLA DIREZIONE

La Direzione di Ai Engineering promuove attivamente una cultura organizzativa orientata alla sicurezza delle informazioni. Tale impegno si manifesta nella definizione di obiettivi chiari, nell'allocazione delle risorse necessarie, nella diffusione della presente Politica e nella verifica costante dell'efficacia del sistema. La Direzione assume un ruolo guida nel promuovere comportamenti responsabili e nel garantire che tutti i livelli dell'organizzazione condividano la responsabilità della protezione delle informazioni. Essa si impegna altresì a sostenere il miglioramento continuo del ISMS, garantendo che i risultati delle valutazioni, degli audit e delle segnalazioni contribuiscano all'evoluzione e al rafforzamento del sistema.

13 RUOLI, RESPONSABILITÀ E AUTORITÀ

Il governo del Information Security Management System (ISMS) è affidato alla Direzione, che assegna specifici compiti e responsabilità alle funzioni aziendali coinvolte. Un Responsabile ISM (ISM Manager) ha il compito di coordinare e mantenere il sistema. I Responsabili di funzione sono tenuti ad applicare le misure di sicurezza nei propri ambiti operativi, mentre i referenti IT e privacy forniscono supporto tecnico e normativo per la gestione dei rischi e degli incidenti. Tutti i dipendenti e collaboratori sono chiamati a conoscere e rispettare le regole e le procedure aziendali in materia di sicurezza.

14 ECCEZIONI

Eventuali deroghe alla presente Politica devono essere autorizzate in via straordinaria dalla Direzione, solo in presenza di motivazioni documentate e fondate su esigenze operative non altrimenti gestibili. Ogni eccezione deve essere formalmente registrata e sottoposta a verifica periodica, al fine di valutare la permanenza delle condizioni che ne hanno determinato l'approvazione.

15 VIOLAZIONI E SANZIONI

La violazione delle disposizioni contenute nella presente Politica o nei documenti a essa collegati può comportare l'applicazione di provvedimenti disciplinari e/o legali. Le infrazioni da parte di personale interno o soggetti esterni sono considerate gravi

inadempienze contrattuali e potranno determinare la risoluzione del rapporto di lavoro o collaborazione, oltre a eventuali segnalazioni alle autorità competenti nei casi previsti dalla legge.

16 SEGNALAZIONE DELLE VIOLAZIONI

Tutti i soggetti che rilevino o sospettino violazioni della presente Politica, vulnerabilità, incidenti o anomalie riguardanti la sicurezza delle informazioni, sono tenuti a segnalarle tempestivamente al Responsabile ISM, attraverso l'indirizzo e-mail dedicato: irt@aigroup.it.
Le segnalazioni vengono trattate in modo confidenziale e analizzate per attivare, se necessario, le opportune misure correttive e preventive.

17 VALIDITÀ, REVISIONE E APPROVAZIONE

La presente Politica è approvata formalmente dalla Direzione di Ai Engineering e viene sottoposta a riesame almeno una volta all'anno o in occasione di eventi che comportino cambiamenti significativi nel contesto normativo, organizzativo o tecnologico. Ogni nuova versione sostituisce quella precedente e viene comunicata tempestivamente a tutti i soggetti interessati, diventando vincolante per l'intera organizzazione e per i suoi partner esterni. A supporto della tracciabilità, ogni revisione è accompagnata da un'indicazione di versione, data di approvazione e riferimenti ai responsabili della redazione e del controllo.

18 RIFERIMENTI NORMATIVI E DOCUMENTALI

La presente Politica si ispira e si conforma ai seguenti riferimenti:

- Norma ISO/IEC 27001:2022 – Sistemi di gestione per la sicurezza delle informazioni;
- Regolamento UE 2016/679 (GDPR) – Protezione dei dati personali;
- Normativa nazionale vigente in materia di privacy e sicurezza (D.Lgs. 196/2003 e s.m.i.);
- Altri standard applicabili contrattualmente o per settore (es. ISO 9001).

Eventuali ulteriori documenti di dettaglio (procedure, istruzioni operative, piani di sicurezza) costituiscono parte integrante del sistema di gestione e sono disponibili presso il sistema documentale aziendale.

Torino, 09/01/2025
Ai Engineering s.r.l.

End