# Politica della Sicurezza delle Informazioni

| Data emissione | Versione | Descrizione | Autore |
|---|---|---|---|
| 18.06.25 | V.1 | Prima stesura per cambio versione anno 2022 | RSI |

| | Idoneità | Adeguatezza |
|---|---|---|
| **Riesame** | RSGSI 18/06/25 | Amm. Unico 18/06/25 |
| **Approvazione** | RSGSI 18/06/25 | Amm. Unico 18/06/25 |

**Riferimenti ISO27001:2022**

§ 5.2 – Politica

# Sommario

## 1. Scopo e ambito di applicazione

La presente Politica per la Sicurezza delle Informazioni definisce i principi e gli impegni di INEO Srl per la protezione, la riservatezza, l'integrità e la disponibilità delle informazioni trattate nell'ambito delle proprie attività.
Essa costituisce il riferimento strategico e operativo per il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), istituito secondo la norma ISO/IEC 27001:2022 e applicato a tutti i processi, sistemi e persone coinvolte nel trattamento delle informazioni aziendali e dei dati dei clienti.

La Politica si applica a:

- tutte le unità organizzative e i dipendenti di INEO;
- i collaboratori esterni, partner e fornitori che accedono ai sistemi informativi;
- tutte le informazioni gestite, indipendentemente dal formato (digitale, cartaceo o verbale).

## 2. Principi generali

INEO riconosce che la sicurezza delle informazioni è un fattore strategico per la tutela del proprio know-how, per la fiducia dei clienti e per la conformità normativa.
Pertanto, la gestione della sicurezza si basa sui seguenti principi fondamentali:

1. **Riservatezza:** accesso alle informazioni consentito solo a persone autorizzate e secondo il principio del "need to know".
2. **Integrità:** garanzia che le informazioni siano accurate, complete e protette da modifiche non autorizzate.
3. **Disponibilità:** assicurazione che le informazioni e i sistemi siano accessibili in modo affidabile agli utenti legittimati quando necessario.
4. **Conformità:** rispetto delle leggi, normative e standard applicabili (ISO/IEC 27001, GDPR, eIDAS, ETSI, EBA, AML, AgID).
5. **Responsabilità e consapevolezza:** ogni persona in INEO è responsabile della protezione delle informazioni che gestisce.
6. **Miglioramento continuo:** il SGSI è oggetto di costante revisione e aggiornamento per rispondere all'evoluzione delle minacce e dei requisiti aziendali.

## 3. Obiettivi della Sicurezza delle Informazioni

Gli obiettivi principali di INEO in materia di sicurezza delle informazioni sono:

1) proteggere i dati aziendali e dei clienti da accessi non autorizzati, perdite o alterazioni;
2) garantire la conformità alle normative e agli standard internazionali;
3) gestire i rischi informativi attraverso un processo strutturato di valutazione e trattamento (rif. §6.1);
4) assicurare la continuità operativa dei servizi digitali erogati;
5) incrementare il livello di consapevolezza e competenza del personale;
6) mantenere la fiducia delle parti interessate grazie a controlli efficaci e verificabili.

## 4. Impegni della Direzione

La Direzione Generale di INEO si impegna a:

- ✧ integrare la sicurezza delle informazioni nei processi aziendali e decisionali;
- ✧ assicurare le risorse necessarie per l'attuazione e il miglioramento del SGSI;
- ✧ promuovere la cultura della sicurezza a tutti i livelli dell'organizzazione;
- ✧ rispettare i requisiti legali, regolamentari e contrattuali;
- ✧ riesaminare periodicamente l'efficacia del SGSI e i risultati conseguiti;
- ✧ garantire che il personale sia formato e consapevole delle proprie responsabilità;
- ✧ assicurare la corretta gestione degli incidenti di sicurezza e delle non conformità;
- ✧ mantenere aggiornato il SoA e le relative misure di controllo in base ai rischi emergenti.

La Direzione nomina il Responsabile Sicurezza delle Informazioni quale figura incaricata di coordinare il sistema, monitorarne l'efficacia e riferire direttamente alla Direzione.

## 5. Comunicazione e diffusione

La Politica per la Sicurezza delle Informazioni è:

1) **pubblicata** sul portale intranet aziendale e disponibile a tutto il personale;
2) **comunicata** via mail in caso di cambiamenti sostanziali;
3) **trasmessa** ai fornitori e partner rilevanti come parte delle clausole contrattuali;
4) **diffusa** ai clienti e alle autorità competenti su richiesta.

Eventuali revisioni o aggiornamenti sono comunicati tempestivamente a tutto il personale interessato.

## 6. Riesame e aggiornamento

La presente Politica è riesaminata **almeno annualmente** o in occasione di:

- variazioni significative nel contesto aziendale o normativo;
- modifiche al campo di applicazione del SGSI;
- esiti di audit, incidenti o non conformità rilevanti;
- decisioni strategiche della Direzione Generale.