Politica di sicurezza delle informazioni

1	07/10/2026	Aggiornamento loghi	Pubblico	MBR	RSGISI (SGI)	ARU (Tech. Director)
0	01/07/2025	Prima emissione	Pubblico	MBR	RSGISI (SGI)	ARU (Tech. Director)
REV.	**DATA**	**DESCRIZIONE**	**CLASSIFICAZIONE**	**PREPARATO**	**CONTROLLATO**	**APPROVATO**

1. Scopo

Incico S.p.A., con il presente documento, definisce la politica di sicurezza delle informazioni al fine di proteggere adeguatamente i dati, le informazioni e i sistemi informativi aziendali di supporto ed elaborazione, nonché ottemperare al requisito *5.2* dello Standard ISO/IEC 27001:2022.
La presente politica è un documento di alto livello. Da esso discendono e si ispirano ulteriori politiche specifiche e procedure tecniche sempre inerenti alla Sicurezza delle Informazioni fondamentali per il mantenimento di un Sistema di Gestione ISO 27001. Tali politiche e procedure di dettaglio potranno essere, a seconda del loro contesto e sensibilità, limitate a gruppi limitati di persone.

2. Obiettivi

Vista l'eterogeneità dei settori di intervento, l'azienda si pone come obiettivo primario l'***armonizzazione della protezione delle informazioni***, ovvero di misure minime di sicurezza volte alla non frammentazione della protezione se non motivata da ragioni specifiche, quali:

- Informazioni sottoposte a condizioni di riservatezza richieste da norme o regolamenti nazionali o di diritto comunitario;
- Informazioni sottoposte a condizioni di riservatezza richieste da soggetti privati in virtù di clausole contrattuali specifiche;
- Progetti legati a difesa, infrastrutture pubbliche o altre aree sensibili;
- Informazioni aziendali strategiche, di ricerca e sviluppo, proprietà intellettuale;
- Informazioni la cui perdita o alterazione potrebbe comportare un pregiudizio economico significativo, grave perdita reputazionale, sanzioni o perdite di opportunità di business;
- Progetti tecnici e ingegneristici in cui anche la minima modifica non autorizzata può compromettere la qualità del prodotto o la sicurezza dell'impianto/progetto.

L'armonizzazione della protezione è guidata dai tre principi cardine della Sicurezza delle Informazioni:

- **Riservatezza**: garantire che le informazioni siano accessibili esclusivamente a soggetti autorizzati;
- **Integrità**: salvaguardare l'accuratezza e la completezza delle informazioni;
- **Disponibilità**: assicurare che le informazioni siano accessibili agli utenti autorizzati nel momento in cui ne abbiano necessità.

2.1 Principi di sicurezza fisica e ambientale

Incico S.p.A. ritiene fondamentale garantire che le informazioni e i sistemi dell'azienda siano protetti da minacce fisiche e danni ambientali. Ciò implica adottare misure per limitare l'accesso non autorizzato agli edifici, server, e altre infrastrutture critiche. Tra le misure adottate, vi sono il controllo degli accessi fisici, la videosorveglianza, e l'impiego di dispositivi di protezione.

La Società si impegna a tener conto delle minacce ambientali, come incendi, allagamenti o altre calamità naturali, implementando soluzioni di protezione, ad esempio sistemi antincendio e backup energetici, per garantire la protezione continua delle operazioni aziendali.

2.2 Principi di gestione operative delle comunicazioni

Incico S.p.A. si impegna ad assicurare una gestione operativa efficace che tutte le attività dell'infrastruttura informatica dell'azienda siano svolte in modo sicuro, efficiente e conforme ai requisiti di sicurezza. Questo include, segnatamente, la gestione appropriata delle risorse, la manutenzione regolare dei sistemi, la pianificazione delle operazioni quotidiane per minimizzare i rischi e l'utilizzo di tecnologie appropriate, insieme a procedure definite per la gestione e trasmissione delle informazioni.

2.3 Controllo degli accessi

Incico S.p.A. considera il controllo degli accessi logici e fisici un principio chiave per garantire che esclusivamente il personale autorizzato possa accedere a informazioni sensibili e a sistemi critici.
La corretta gestione delle credenziali, l'implementazione di autenticazioni multiple ove possibile, e la limitazione dei permessi in base ai ruoli e alle responsabilità all'interno dell'organizzazione sono essenziali per l'accesso a progetti, dati tecnici, e altre risorse strategiche.

2.4 Gestione della continuità operativa

La gestione della continuità operativa è necessaria affinché l'Azienda sia in grado di mantenere le proprie attività anche in caso di interruzioni o eventi catastrofici.
L'adozione di un piano di continuità operativa permette di assicurare che le attività critiche possano continuare anche in situazioni di emergenza. Questo implica l'implementazione di backup regolari dei dati, piani di ripristino in caso di disastro, e l'identificazione di fornitori e risorse alternative che possano supportare le operazioni in caso di guasti.

3. Leadership

Con la presente politica la Direzione, a nome di Incico S.p.A. esprime il proprio impegno a:

- Effettuare un monitoraggio continuo dei processi per assicurare la protezione delle informazioni all'interno del Sistema di Gestione della Sicurezza delle Informazioni.
- Favorire un miglioramento costante del suddetto sistema.
- Documentare, analizzare e investigare tempestivamente ogni violazione o incidente di sicurezza, identificando le cause principali e adottando le misure correttive necessarie.
- Promuovere una formazione continua e una costante sensibilizzazione dei dipendenti sulla sicurezza delle informazioni, evidenziando il valore del loro contributo per il buon funzionamento del sistema.

- Gestire i rischi legati alla conservazione e al trattamento delle informazioni, mantenendoli entro soglie accettabili.

4. Distribuzione e comunicazione

Il presente documento è pubblico, liberamente consultabile dalle parti interessate e reso disponibile alla intera popolazione aziendale.

FIRMATO

Data

08/09/2025

incico s.p.A.
Antonello Ruttilio
(Direttore Tecnico)