Allegato

Politica per la gestione dei servizi

Storicità del documento

Major Release	Azione	Funzione Aziendale	Data
1	Redatto	COMP, PROCE	04/12/2025
	Verificato	COMP	04/12/2025
	Pubblicato	PROCE	09/12/2025

Storico delle modifiche

Major Release	Minor Release	Data di pubblicazione	Motivo della revisione
1	0	09/12/2025	Prima emissione, sostituisce ed integra la precedente PKG_COMP_AL07

Politica per la Gestione dei Servizi

Come Direzione di Kirey S.r.l. e Insirio S.r.l. (da qui in avanti "**Kirey**") intendiamo proteggere le informazioni da un ampio spettro di minacce allo scopo di assicurare la continuità delle nostre attività, minimizzare i rischi, garantire il ritorno dagli investimenti, le opportunità di business, il rispetto delle leggi e la redditività. Tutti i dati e le relative elaborazioni per la gestione delle nostre attività devono essere protetti per garantire che giungano integre a chi deve utilizzarle, che non vadano disperse o peggio ancora che non finiscano nelle mani di concorrenti o di approfittatori.

L'Informazione è un Asset, e come altri Asset materiali o immateriali è un elemento essenziale per l'organizzazione Kirey; come tale, ha anche bisogno di essere tutelata. Le tutele sono tanto più necessarie quanto più l'interconnessione è ampia, cosa che espone l'Informazione ad una più larga varietà di rischi e di vulnerabilità come frodi, spionaggio, vandalismi e incidenti.

Kirey è consapevole della necessità di rendere tutti consapevoli della delicatezza con cui devono essere trattate le Informazioni; perciò, si impegna a condividere gli obiettivi ed i principi della sicurezza delle informazioni. Sulla struttura organizzativa e sui processi in essere in Kirey è stato integrato il Sistema di Gestione dei Servizi ("**SGS**") cioè l'insieme di politiche, processi, procedure, ruoli, responsabilità, risorse e strumenti che permettono a Kirey di gestire il rischio relativo alle informazioni.

In particolare, con l'implementazione di questo sistema:

- Viene gestita un'analisi dei rischi;
- I rischi così' individuati vengono trattati sulla base di criteri di accettazione, preservando il rispetto delle leggi dello Stato ed i requisiti contrattuali.
- Pertanto, sulla base dei criteri prestabiliti:
  - i rischi vengono accettati consapevolmente al fine di gestirli;
  - vengono evitati i rischi non permettendo azioni/attività che potrebbero essere causa dei rischi stessi;
  - se del caos, i rischi vengono trasferiti a terze parti.
- Viene alimentata una cultura tesa a rendere tutti consapevoli della necessità di operare responsabilmente mediante formazione a tuttii livelli;
- Vengono introdotte specifiche attività di controllo e precauzioni contro i disastri;
- Vengono assunti adeguati provvedimenti e best practices a seguito di ogni rischio di violazione o violazione;
- A ciò si aggiunge:
  - Il monitoraggio di tutti gli eventi con la verifica dell'efficacia dei controlli prescritti ed il successivo riesame;
  - L'attivazione di azioni di miglioramento;
  - La gestione della documentazione e delle registrazioni di sistema;
  - L'addestramento di tutto il personale per conseguire competenza e consapevolezza sulle problematiche della sicurezza delle informazioni;
  - Audit interni per verificare che i controlli sono efficaci, gli obiettivi dei controlli vengono raggiunti e che le procedure vengono applicate: in sintesi che il SGS sia conforme alla norma di riferimento ISO/IEC 27001:2022 ed alla ISO/IEC 20000-1:2018;
  - Il Riesame della Direzione;
  - Il miglioramento con Azioni Correttive e di Miglioramento.

Per garantire l'efficacia del SGS sono assegnate le seguenti responsabilità:

- **Direzione**
  - Definizione del perimetro e il dominio degli Asset da proteggere;
  - Riesame periodico dello stato di sicurezza delle informazioni oltre che dell'efficacia della presente politica;
  - Approvazione delle azioni di miglioramento proposte.
- **Responsabile SGS**
  - Valutazione de rischi cui possono essere esposti gli Asset;
  - Definizione, implementazione e monitoraggio dei controlli necessari per la gestione dei servizi;
  - Coordinamento delle attività di miglioramento continuo del SGS.
- **Responsabile SGSI**
  - Registrazione di tutte le minacce verificate e gli incidenti di sicurezza;
  - Pianificazione e implementazione di nuovi controlli atti a mitigare i rischi;
  - Avvio delle azioni correttive preventive in caso di non conformità.
- **Tutti i Dipendenti**
  - Rispetto delle autorizzazioni e alle procedure adottate dalla società;
  - Segnalazione tempestiva al Responsabile SGSI di eventuali minacce e/o anomalie riscontrate.