



POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Revisione:	1.0
Data di revisione:	26/11/2024
Redatto da:	RGSI
Approvato da:	DIREZIONE
Livello di Riservatezza	PUBBLICO



Cronologia delle revisioni

Data	Revisione	Creata da	Descrizione della modifica
26/11/2024	1.0	RGSI	Prima emissione
11/07/2025	2.0	RGSI	Integrazione normativa

Sommario

1.	INTRODUZIONE	3
2.	OBIETTIVO	3
3.	AMBITO DI APPLICAZIONE	3
4.	PRINCIPI DELLA SICUREZZA DELLE INFORMAZIONI	3
5.	RUOLI E RESPONSABILITÀ	4
6.	VALUTAZIONE DEI RISCHI	4
7.	CONTROLLI DI SICUREZZA	4
8.	CONFORMITÀ LEGALE E NORMATIVA	5



1. Introduzione

La sicurezza delle informazioni è essenziale per la protezione degli asset aziendali, della reputazione e del successo dell'organizzazione. Questa politica definisce i principi e gli obiettivi per la gestione della sicurezza delle informazioni in conformità con lo standard **ISO 27001**, e include estensioni specifiche per l'**ambiente cloud computing** come indicato dagli standard **ISO 27017** e **ISO 27018**

2. Obiettivo

L'obiettivo della presente politica è proteggere le informazioni aziendali da ogni minaccia, interna o esterna, deliberata o accidentale, e garantire la riservatezza, l'integrità e la disponibilità delle informazioni.

In aggiunta:

- Garantire la protezione dei dati personali memorizzati nel cloud, anche quando gestiti da fornitori terzi ISO 27018.
- Garantire controlli di sicurezza adeguati nei servizi di cloud computing, compresi ambienti multi-tenant, in conformità con la ISO 27017.

3. Ambito di applicazione

Questa politica si applica a tutti i dipendenti, collaboratori, fornitori e terze parti che trattano informazioni aziendali e utilizzano sistemi, reti e risorse informatiche dell'organizzazione, inclusi servizi e infrastrutture cloud.

Si specifica che:

- Le attività di trattamento, elaborazione e conservazione dei dati possono avvenire su piattaforme di cloud computing.
- La posizione geografica dei dati nei cloud provider (attualmente Irlanda) è monitorata



per assicurare conformità alla normativa europea (es. GDPR) (ISO/IEC 27018).

4. Principi della Sicurezza delle Informazioni

L'organizzazione si impegna a proteggere le informazioni seguendo questi principi fondamentali:

- **Riservatezza:** Garantire che le informazioni siano accessibili solo a chi è autorizzato a visualizzarle.
- **Integrità:** Salvaguardare l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione.
- **Disponibilità:** Assicurare che le informazioni ei sistemi siano accessibili e utilizzabili quando necessario.
- Segregazione logica tra tenant (ISO 27017).
- Controllo degli accessi da parte dei fornitori cloud con tracciabilità e registrazione (ISO 27018).

5. Ruoli e responsabilità

- **Direzione Aziendale:** Responsabile del supporto e dell'approvazione della politica sulla sicurezza delle informazioni e dell'allocazione delle risorse necessarie.
- **Responsabile del Sistema di Gestione della Sicurezza delle Informazioni (RGSI):** Responsabile dell'implementazione, del mantenimento e del miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).
- **Dipendenti e Collaboratori:** Devono garantire la **conformità agli standard ISO 27017 e 27018**, in particolare per la protezione dei dati personali, la segregazione degli



ambienti e la trasparenza sulla localizzazione dei dati.

6. Valutazione dei rischi

L'organizzazione effettuerà regolarmente una valutazione dei rischi per identificare, analizzare e gestire i rischi associati alla sicurezza delle informazioni. Verranno adottate misure per ridurre i rischi a un livello accettabile attraverso controlli preventivi, correttivi e di mitigazione, includendo:

- Rischi specifici legati all'utilizzo del cloud computing, come accessi non autorizzati da parte del provider, movimentazione geografica dei dati, o vulnerabilità nei servizi multi-tenant.
- Verranno adottate misure preventive specifiche per il cloud, come richiesto dalla ISO 27017.

7. Controlli di sicurezza

L'organizzazione adotterà e manterrà controlli di sicurezza fisici, logici e organizzativi per proteggere le informazioni aziendali. Tra questi controlli si includono:

- Controllo degli accessi (anche per utenti cloud e provider).
- Crittografia di dati personali memorizzati nel cloud (ISO/IEC 27018).
- Gestione degli incidenti anche su ambienti cloud.
- Backup con garanzia di accessibilità anche su piattaforme cloud.



- Formazione specifica sulla gestione sicura dei dati in ambienti cloud.

8. Conformità Legale e Normativa

L'organizzazione si impegna a:

- Rispettare tutte le normative nazionali e internazionali, inclusa la **GDPR**.
- Assicurare che i **fornitori cloud siano conformi** alle normative sulla protezione dei dati personali.
- **Monitorare la localizzazione geografica dei dati** (attualmente Irlanda), garantendo che il trattamento avvenga in paesi con adeguate garanzie legali.

9. Verifica e Riesame

La politica sulla sicurezza delle informazioni sarà regolarmente verificata e riesaminata per garantirne l'efficacia e l'allineamento con i cambiamenti normativi, tecnologici e aziendali. Verranno condotti audit interni per valutare la conformità al Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

10. Conseguenze delle Violazioni

Le violazioni della presente politica o delle procedure associate saranno trattate seriamente e potranno comportare azioni disciplinari, inclusa la risoluzione del contratto di lavoro o azioni legali.

11. Miglioramento Continuo

L'organizzazione si impegna al **miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni** per adattarsi a **nuove minacce, opportunità e sviluppi**



tecnologici.

Tale impegno include anche:

- La revisione costante delle pratiche di sicurezza nei contesti cloud.
- L'adozione di misure e tecnologie innovative per la protezione dei dati personali in ambienti cloud.
- La collaborazione con fornitori che dimostrano un impegno documentato nella **conformità agli standard ISO/IEC 27017 e ISO/IEC 27018**.
- L'aggiornamento regolare di contratti, accordi e procedure interne in linea con l'evoluzione normativa, tecnologica e delle minacce informatiche.