

Politica per la Qualità e la Sicurezza delle Informazioni

INFORMAZIONI DOCUMENTO:

Versione	1.0	Classificazione	Esterno
Data emissione	16/12/2025	Data ultimo aggiornamento	16/12/2025
Responsabile emissione	RSGI	Responsabile approvazione	La Direzione

INDICE

1. Premessa.....	3
2. Ambito di applicazione.....	3
3. Principi e Motivazioni.....	3
4. Impegno e Responsabilità.....	4
5. Violazione della politica.....	4
6. Segnalazione di incidenti di sicurezza o vulnerabilità	5
7. Entrata in vigore	5

1. Premessa

La Direzione definisce la presente Politica per la Qualità e la Sicurezza delle Informazioni quale riferimento strategico per lo sviluppo, l'attuazione e il miglioramento continuo del Sistema di Gestione Integrato aziendale, in conformità alle norme ISO 9001:2015 e ISO 27001:2022.

L'organizzazione riconosce la qualità dei servizi e la protezione delle informazioni come elementi fondamentali per la soddisfazione dei clienti, la continuità operativa, la reputazione aziendale e la sostenibilità del proprio modello di business.

La presente politica per la qualità e la sicurezza delle informazioni si applica in modo unitario e coerente a tutte le società del Gruppo Stratos garantendo uniformità, trasparenza e omogeneità nei principi, negli impegni e nelle responsabilità che il Gruppo si assume.

2. Ambito di applicazione

La presente Politica si applica in modo unitario e coerente a tutte le società del Gruppo Stratos, ovvero Stratos S.r.l. e Stratos Analytics S.r.l., a tutte le attività aziendali, al personale interno, ai collaboratori, ai partner e ai fornitori coinvolti nell'erogazione dei servizi e nella gestione delle informazioni.

Essa riguarda in particolare:

- la qualità dei servizi offerti ai clienti;
- la sicurezza delle informazioni aziendali e dei clienti;
- la gestione dei processi operativi, tecnologici e organizzativi;
- il rispetto delle normative applicabili e degli obblighi contrattuali.

3. Principi e Motivazioni

La Politica per la Qualità e la Sicurezza delle Informazioni si fonda sui seguenti principi guida, coerenti con il contesto aziendale, il modello di business e le esigenze degli stakeholder.

Centralità del cliente

L'organizzazione orienta le proprie attività alla soddisfazione dei clienti, assicurando servizi affidabili, competitivi e conformi ai requisiti contrattuali, normativi e di sicurezza delle informazioni.

Centralità delle persone e dei partner

Le competenze delle persone, la collaborazione interna e il rapporto trasparente con fornitori e partner rappresentano elementi fondamentali per la qualità dei servizi, l'innovazione e la sicurezza delle informazioni.

Qualità dei servizi e sicurezza delle informazioni

L'organizzazione si impegna a garantire servizi di qualità proteggendo le informazioni aziendali e dei clienti in termini di riservatezza, integrità e disponibilità, assicurando continuità operativa e gestione proattiva dei rischi.

Miglioramento continuo e conformità normativa

L'organizzazione promuove il miglioramento continuo dei processi, delle competenze e delle prestazioni del sistema di gestione, operando nel rispetto delle normative applicabili, degli standard internazionali e degli obblighi contrattuali, nonché favorendo la resilienza operativa digitale anche in relazione alle esigenze dei clienti soggetti a specifici requisiti regolatori.

4. Impegno e Responsabilità

La Direzione assicura che la qualità dei servizi e la sicurezza delle informazioni siano elementi integrati negli obiettivi aziendali e nei processi operativi, promuovendo un Sistema di Gestione efficace e orientato al miglioramento continuo.

L'organizzazione si impegna a proteggere le informazioni aziendali e dei clienti garantendone:

- **Riservatezza**, assicurando che l'accesso alle informazioni sia consentito esclusivamente ai soggetti autorizzati secondo il principio del minimo privilegio;
- **Integrità**, garantendo accuratezza, completezza e protezione delle informazioni da modifiche o cancellazioni non autorizzate;
- **Disponibilità**, assicurando l'accesso alle informazioni e ai servizi quando necessario per le attività operative e per i clienti.

La Direzione si impegna altresì a:

- garantire la continuità operativa dei servizi offerti;
- garantire un'adeguata ed efficace gestione degli incidenti di sicurezza;
- divulgare e promuovere la cultura della qualità e sicurezza delle informazioni.

La sicurezza delle informazioni rappresenta un fattore abilitante per la continuità operativa, la condivisione controllata delle informazioni e la gestione dei rischi aziendali, tenendo conto anche dell'evoluzione del contesto tecnologico, organizzativo e ambientale.

Tutto il personale, i collaboratori e i partner sono responsabili dell'applicazione delle politiche, delle procedure e delle misure di sicurezza previste dall'organizzazione.

5. Violazione della politica

Ogni dipendente, fornitore o collaboratore che opera per conto di Stratos è tenuto a rispettare integralmente questa Politica e le procedure operative associate.

Eventuali violazioni dei principi sopra indicati, che comportino la compromissione della Riservatezza, Integrità o Disponibilità delle informazioni, sono trattate con la massima serietà. In funzione della gravità e dell'impatto dell'evento, potranno implicare:

- Attivazione di procedimenti disciplinari interni nei confronti dei dipendenti, in conformità con il contratto di lavoro, regolamento aziendale e le normative vigenti;
- Risoluzione dei contratti nei confronti di fornitori o collaboratori esterni per inadempienza degli obblighi di sicurezza;
- Eventuali azioni legali per danni causati

Per garantire una gestione tempestiva e confidenziale di qualsiasi potenziale minaccia, vulnerabilità o incidente, invitiamo tutti gli stakeholder a utilizzare il seguente canale prioritario:

compliance@gruppostratos.com

6. Segnalazione di incidenti di sicurezza o vulnerabilità

Se si sospetta o si ha conoscenza di una violazione della sicurezza, di una vulnerabilità o di un Data Breach che coinvolge sistemi o informazioni, si prega di utilizzare i seguenti link per le segnalazioni:

-Incidenti di sicurezza asset fisici ed informativi: incident@gruppostratos.com

-Violazioni di dati personali:

- Stratos S.r.l. <https://www.privacylab.it/dataBreach.phtml?step=submitreport&ckey=pe8-8x9-6e8>
- Stratos Analytics: <https://www.privacylab.it/dataBreach.phtml?step=submitreport&ckey=re8-8y9-6e7>

Tutte le segnalazioni saranno gestite dal Responsabile Sistema Gestione Integrata (RSGI).

La Direzione si impegna a riesaminare tale politica annualmente, al fine di confermarne l'attualità e di formulare gli obiettivi di miglioramento coerenti con essa. La Direzione si impegna altresì a comunicare e applicare la presente Politica all'interno dell'organizzazione ed a renderla disponibile alle parti interessate rilevanti, compresi collaboratori e fornitori che prestano servizi per conto della società.

7. Entrata in vigore

La presente Politica è un documento pubblico, reso disponibile alle parti interessate, ed entra in vigore dalla data di approvazione fino a successivo aggiornamento o revisione, con efficacia a partire dalla comunicazione ufficiale effettuata a tutti i Destinatari su sito Internet ed intranet aziendale.