

	Politica per la sicurezza delle informazioni e per la gestione del servizio	PSI-SMS
	documento pubblico- riproduzione vietata	

La società **Principium Srl**, nell'ottica di ottemperare ai disposti normativi della Norma UNI EN ISO/IEC 27001, oltrechè al fine di gestire al meglio i propri servizi, secondo le indicazioni della Norma UNI ISO/IEC 20001, intendendo salvaguardare e migliorare la gestione del proprio business, ha deciso di mettere in atto una serie di misure tecniche, organizzative e procedurali, volte da un lato a garantire la sicurezza delle informazioni, salvaguardandole da violazioni che possano pregiudicarne disponibilità, integrità, autenticità e riservatezza, dall'altra a mantenere attivo e migliorare il proprio sistema di gestione dei servizi.

La Direzione stabilisce pertanto di proteggere le informazioni e in particolare la loro:

1. Riservatezza, assicurando che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
2. Integrità, salvaguardando l'informazione da modifiche non autorizzate;
3. Disponibilità, assicurando che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetture associati quando ne fanno richiesta;
4. Autenticità, assicurando la provenienza affidabile dell'informazione;

Per far ciò si attua una rigorosa politica di Controlli, finalizzata ad assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati.

La politica per la sicurezza delle informazioni e per il service management di **Principium Srl** si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutte le attività, i processi e le risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.

Essa si collega strettamente al Piano obiettivi annuale della società.

Nell'ambito della gestione dei servizi offerti da **Principium Srl**, attraverso la propria infrastruttura tecnologica, l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione dell'SI-SMS, ci rende confidenti:

- di aver incaricato partner affidabili, nell'ambito del trattamento del nostro patrimonio informativo;
- di confermare un'elevata immagine aziendale;
- osservare in modo attento i Service Level Agreement stabiliti con i clienti;
- nella piena soddisfazione del cliente;
- del completo rispetto delle normative vigenti e degli standard internazionali di sicurezza, in special modo in relazione al trattamento dei dati personali ex Reg Eu 679/2016 e suo recepimento in ambito nazionale;
- del fatto che collaborare con le Autorità non è solo un dovere ma una opportunità di mostrare il nostro livello di adeguamento alle normative vigenti, in particolar modo in caso di attacco ai sistemi informatici, con accesso a dati di Interessati;
- di rispondere pienamente ai requisiti contrattuali sottoscritti coi clienti.

Tutto ciò rappresenta formale impegno di **Principium Srl** nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività nonché una gestione controllata dei servizi erogati.

La politica della sicurezza delle informazioni di **Principium Srl** ha i seguenti obiettivi, che vengono dettagliati nei Piani degli obiettivi aziendali e periodicamente verificati:

	Politica per la sicurezza delle informazioni e per la gestione del servizio	PSI-SMS
	documento pubblico- riproduzione vietata	

- A Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
- B Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
- C Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.
- D Garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, abbiano piena consapevolezza delle problematiche relative alla sicurezza.
- E Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
- F Garantire che ai locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
- G Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
- H Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
- I Garantire la business continuity aziendale, attraverso l'applicazione di procedure di sicurezza stabilite.
- J I. Garantire di comprendere e rispondere adeguatamente ai requisiti contrattuali sottoscritti.
- K m. Garantire l'interesse nell'elevare in modo continuativo la sensibilità del proprio personale sui temi della sicurezza delle informazioni e sul management dei servizi.
- L n. Tendere al miglioramento dei sistemi integrati 27001 e 20000-I.

La politica della sicurezza delle informazioni e del service management viene costantemente aggiornata per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema intranet e specifici canali di comunicazione.

La Direzione è responsabile del sistema di gestione sicura delle informazioni e del service management, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando periodicamente eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business;
- modifiche ai servizi;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni e dei dati.

Roma, 12.01.2026

Approvato dalla Direzione

PRINCIPIUM SRL
Via Meuccio Ruini, 31
00155 ROMA
P.IVA 09428461006