

POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

SCHEMA CONTROLLO DOCUMENTO

IDENTIFICAZIONE

TITOLO: Politica della Sicurezza delle Informazioni

CODICE:

REVISIONI

VERSIONE	DATA EMISSIONE	COMMENTO
1.0	03/11/2023	Prima Emissione
1.1	14/10/2024	rif. alla politica dell'uso di AI.

AUTORIZZAZIONI

REDATTO DA	Alessandro Guglielmi	Responsabile SGSI
VERIFICATO DA	Ernesto Ferrari	Risk/Asset Owner
APPROVATO DA	Giorgio Casanova	Alta Direzione

INTRODUZIONE

Per METEL Srl (d'ora in poi anche "l'Azienda") la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa, responsabile della loro gestione. Questo significa ottenere e mantenere un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) sicuro, nell'ambito del campo di applicazione definito, attraverso il rispetto delle seguenti proprietà:

- ✓ **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
- ✓ **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
- ✓ **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architettonici associati quando ne fanno richiesta;
- ✓ **Controllo:** assicurare che la gestione dei dati e delle informazioni avvenga sempre attraverso processi e strumenti sicuri e testati;
- ✓ **Autenticità:** garantire una provenienza affidabile dell'informazione;
- ✓ **Privacy:** garantire la protezione e il controllo dei dati personali.

Nell'ambito della gestione dei servizi offerti dall'Azienda, attraverso la propria infrastruttura tecnologica, l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione del SGSI, assicura:

- ✓ La garanzia di avere realizzato un sistema affidabile per il trattamento del patrimonio informativo;
- ✓ Un'elevata immagine aziendale;
- ✓ La completa osservanza dei livelli di servizio stabiliti con i clienti;
- ✓ La soddisfazione dei clienti;
- ✓ Il rispetto delle normative vigenti e degli standard internazionali di sicurezza delle informazioni.

Per questo motivo l'Azienda ha sviluppato un SGSI seguendo i requisiti specificati della Norma internazionale ISO/IEC 27001:2022 e dalle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.

AMBITO DI APPLICAZIONE

La Politica per la Sicurezza delle Informazioni dell'Azienda si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa dei servizi ai clienti, incluso l'impiego di soluzioni d'intelligenza artificiale regolamentate da apposite politiche e istruzioni operative alle quali si rimanda.

PRINCIPI GUIDA

La nostra organizzazione opera per fronteggiare in modo efficace il contesto competitivo e per mantenere e rafforzare la propria posizione sul mercato, in un'ottica di crescita, che impone un'attenzione sempre maggiore alla sicurezza delle informazioni e dei beni aziendali. Per l'Azienda il significato di sicurezza è ampio e comprende l'insieme delle condizioni che assicurano non solo un luogo di lavoro privo di rischi per la vita e la salute delle sue persone, ma al tempo stesso riducono ad un livello accettabile il rischio di deterioramento o perdita di beni materiali od immateriali quali le informazioni, nonché i rischi relativi alla continuità operativa.

E' stato definito e messo in atto un SGSI in grado sia di identificare tempestivamente che di prevenire quei rischi che possono compromettere la capacità di fornire i prodotti/servizi richiesti dal mercato, nonché di elaborare piani per la gestione delle minacce e delle vulnerabilità.

Un SGSI moderno ed efficace non può nella limitarsi alla reazione agli eventi dannosi, ma al contrario si basa sulla prevenzione. Il valore aggiunto della sicurezza delle informazioni in azienda è dato dalla capacità di agire prima che un evento dannoso si verifichi. Questa condizione ci rende tutti responsabili nel garantire, tramite la maturità e il buon senso dei nostri comportamenti, il raggiungimento di un elevato livello di efficienza ed efficacia nei processi di gestione della sicurezza delle informazioni.

La conoscenza delle regole di sicurezza delle informazioni, unita ad un atteggiamento personale proattivo applicato sistematicamente alla normale attività lavorativa, rende riconoscibili e concreti i risultati di questo impegno aziendale. La presente Politica rappresenta l'impegno dell'organizzazione 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.

La Politica per la sicurezza delle informazioni si ispira ai seguenti principi:

- 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 l'accesso alle sedi ed ai singoli 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 Continuità Operativa attraverso l'applicazione di procedure di sicurezza stabilite.

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

OBIETTIVI

Coerentemente con i principi guida sopra enunciati, l'azienda definisce i seguenti obiettivi generali che devono essere perseguiti in tutti i processi dell'azienda:

- **Gestire la sicurezza delle informazioni**, definendo adeguati obiettivi e traguardi, mettendo a disposizione idonee risorse, predisponendo specifiche politiche e procedure di sicurezza da attuare nei singoli dipartimenti, garantendo sempre la piena conformità con i requisiti legali e normativi;
- **Comunicare** politiche, obiettivi e traguardi per la sicurezza delle informazioni affinché vi sia una reale condivisione e unità d'intenti sui comportamenti da assumere;
- **Minimizzare** le condizioni di rischio e **prevenire** le vulnerabilità che espongono le persone, i beni e il business a minacce, garantendo gli standard e gli obiettivi aziendali, la competitività e l'immagine del marchio e dell'azienda;
- **Coinvolgere** tutto il personale interno e quello dei fornitori tramite attività di informazione, formazione ed addestramento finalizzate ad accrescere conoscenza, competenza e consapevolezza sugli aspetti di sicurezza delle informazioni sia nella gestione delle attività quotidiane sia in caso di incidenti che possano compromettere la continuità aziendale;
- **Garantire** in caso di emergenze e crisi un rapido ritorno alla normale operatività,

contenendo i danni e le perdite, tutelando le persone e il patrimonio aziendale;

- **Monitorare** i processi interni per verificare con continuità l'adeguatezza del sistema ed individuare le possibili azioni di miglioramento;
- **Migliorare** le prestazioni di sicurezza ed il sistema di gestione della sicurezza delle informazioni per allinearle ai cambiamenti globali e alle mutate esigenze aziendali e normative.

I principi enunciati e gli obiettivi definiti devono diventare parte integrante della nostra attività quotidiana.

RESPONSABILITA' DELLA POLITICA DI SICUREZZA

La Direzione è responsabile del SGSI, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- ✓ Evoluzioni significative del business;
- ✓ 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.

La responsabilità di proteggere le persone e le risorse aziendali non può essere demandata ad altri. Tutti coloro che gestiscono, operano ed esercitano attività di controllo nei processi aziendali devono garantire un adeguato livello di protezione utilizzando gli strumenti e le risorse messe a disposizione dall'azienda.

I responsabili di ciascuna funzione e dipartimento devono quindi assicurare che la presente Politica di Sicurezza delle Informazioni sia compresa e attuata da tutto il personale interno e dai fornitori coinvolti.

Milano, 14/10/2024

La Direzione Generale



La direzione
METEL S.R.L.
Via Montefeltro, 6
20156 Milano
Partita IVA 11036210156