POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

La presente Politica si applica a tutto il personale interno o esterno, alle aziende partner, ai fornitori e a chiunque altro che, direttamente o indirettamente, entra in contatto con le informazioni di Motus ml S.r.l. SB (di seguito Moutus ml).

In conformità ai contenuti del Manuale della Sicurezza delle Informazioni, il presente documento riassume la Politica aziendale fondata su una serie di principi volti a garantire un adeguato livello di sicurezza dei dati e delle informazioni.

Il Sistema di Gestione per la Sicurezza delle Informazioni di Motus ml definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sotto elencati requisiti di sicurezza di base:

- **Disponibilità**: ovvero, garantire l'accesso alle informazioni e ai servizi di rete da parte degli utenti autorizzati nel momento in cui lo richiedono;
- **Riservatezza**: ovvero, garantire la prevenzione di accessi abusivi o non autorizzati alle informazioni, ai servizi e ai sistemi;
- **Integrità**: ovvero, garantire che le informazioni non siano state alterate da incidenti o abusi;
- **Resilienza**: ovvero la capacità di un sistema di adattarsi ai cambiamenti.

La mancanza di adeguati livelli di sicurezza può influire sulla reputazione aziendale, sulla violazione di impegni contrattuali con il cliente e infine sulla violazione delle normative vigenti che possono generare ingenti danni di natura economica e finanziaria. L'Azienda identifica le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo considerando altresì il rischio delle informazioni associato all'utilizzo dei servizi cloud. L'analisi del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare da un incidente dovuto alla mancata applicazione di misure di sicurezza e quale sia la realistica eventualità del verificarsi dei rischi identificati. I risultati di questa valutazione determinano le azioni necessarie per mitigare i rischi individuati e le misure di sicurezza più idonee.

A tali fini vengono definiti i seguenti obiettivi di sicurezza:

- Garantire l'integrità, la confidenzialità e la disponibilità delle informazioni trattate;
- Proteggere i dati aziendali da accessi non autorizzati, perdite, furti o danni accidentali;
- Monitorare i livelli di sicurezza presenti nell'organizzazione;
- Definire le regole comportamentali e i principi di utilizzo degli strumenti di lavoro;
- Sensibilizzare e formare il personale sull'importanza della sicurezza delle informazioni;
- Assicurare la conformità alle normative vigenti in materia di trattamento dei dati personali, i diritti della proprietà intellettuale, legge sulla criminalità informatica, sicurezza sul posto di lavoro, etc.;
- Garantire il monitoraggio e controllo delle attività svolte nel pieno rispetto dei principi di privacy e tutela delle informazioni personali;
- Delineare i principi di gestione degli incidenti e delle azioni di ripristino.

Al fine di garantire il raggiungimento degli obiettivi fissati, la Società ha definito i seguenti principi generali di sicurezza da adottare nell'ambito di tutti i processi e delle attività svolte dal personale interno e dai propri stakeholders.

- L'implementazione ed il rispetto delle politiche e delle misure di sicurezza in tutti gli ambiti organizzativi, procedurali e tecnologici, compresi i servizi in cloud, in modo omogeneo rispetto agli obiettivi definiti;
- L'adeguata attribuzione di compiti e responsabilità all'interno dell'Azienda per l'attuazione delle politiche;
- La verifica (nell'ambito dell'analisi del rischio informatico) del livello di efficacia delle misure realizzate;

- Il più ampio coinvolgimento di tutto il personale per l'istituzione, l'attuazione, il mantenimento e il miglioramento continuo del Sistema di gestione della sicurezza dell'informazione e il continuo miglioramento dei servizi erogati.

L'organizzazione si impegna a rispettare le leggi, i regolamenti e gli standard applicabili, e a sensibilizzare il personale sull'importanza della sicurezza delle informazioni attraverso attività di formazione. Vengono inoltre implementati controlli per gestire i rischi connessi alla sicurezza delle informazioni attraverso un approccio sistematico volato a identificare, valutare e mitigare i rischi legati alla sicurezza delle informazioni, seguendo le migliori pratiche internazionali.

Nell'attuazione della politica la Direzione fornisce il supporto e le risorse necessarie per l'implementazione, promuovendo una cultura aziendale orientata alla sicurezza delle informazioni. Il Responsabile della Sicurezza delle Informazioni (CISO) supervisiona l'applicazione delle misure di sicurezza, monitorando e valutando periodicamente l'efficacia del sistema di gestione della sicurezza delle informazioni. Infine, dipendenti e collaboratori sono chiamati a rispettare le procedure stabilite e a segnalare tempestivamente eventuali incidenti di sicurezza.

Per garantire la conformità alla norma ISO/IEC 27001 e ad altri requisiti applicabili, vengono effettuati audit periodici. Eventuali non conformità rilevate saranno gestite attraverso azioni correttive e preventive. La politica è comunicata a tutte le parti interessate, e l'organizzazione promuove programmi di formazione e sensibilizzazione per rafforzare la cultura della sicurezza delle informazioni.

Il presente documento è oggetto di revisione almeno una volta all'anno, o ogni volta che si verifichino cambiamenti significativi nei processi aziendali, nei rischi o nei requisiti normativi. Tale revisione consente di mantenere il documento sempre aggiornato e pertinente alle esigenze dell'organizzazione.

Questa politica è stata approvata dalla Direzione e rappresenta un impegno per tutti i dipendenti e collaboratori.

Milano, 30.09.2024

Giacomo Ziffer

Per Motus ml S.r.l. SB.