



Politica della sicurezza delle informazioni

Rev	Descrizione revisione	Data	Autore	Approvato da	Distribuito a
1	Prima stesura	01 Dic 2023	Roberto Sbravati	Roberto Sbravati	Tutti

ATTENZIONE: Il presente documento è di proprietà della Società Frog Learning srl.
Ogni riproduzione, divulgazione in toto o in parte deve essere autorizzata dalla Società stessa

La direzione di Frog Learning Srl, ha definito la presente Politica per la protezione delle Informazioni e si impegna a:

- mantenerla attiva garantendone periodicamente la revisione e l'aggiornamento,
- garantire le risorse necessarie per l'efficace protezione delle informazioni,
- definire gli obiettivi in materia di sicurezza delle informazioni,
- divulgarla a tutti i livelli della propria organizzazione.

L'applicazione del sistema di gestione richiede la piena partecipazione, l'impegno e l'interazione di tutte le risorse umane e tecnologiche.

Tutti soggetti che operano all'interno della Azienda per il conseguimento degli obiettivi Aziendali, sono tenuti, senza eccezione, all'osservanza della presente politica nel trattamento di dati.

Lo scopo è quello di:

- I. garantire la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle proprie attività, in accordo con quanto indicato nello standard ISO/IEC 27001 e nelle linee guida ISO/IEC 27002.
- II. garantire la tutela e la protezione dei dati in accordo con le indicazioni fornite dal Regolamento europeo in materia di protezione dei dati personali (GDPR 679/16).
- III. garantire l'attivazione di un processo continuo, che permetta il controllo e l'adeguamento ai cambiamenti del management, ambientali, di business e legali a cui l'azienda può andare incontro.

È quindi necessario assicurare:

- IV. la confidenzialità dei dati, ovvero i dati devono essere accessibili solo a chi è all'uopo autorizzato.
- V. L'integrità dei dati, ovvero garantire la precisione e la completezza dei dati e dei metodi per la loro elaborazione.
- VI. La disponibilità dei dati, ovvero che solo gli utenti autorizzati possano effettivamente accedere ai dati nel momento in cui lo richiedono. La comunicazione e la diffusione delle dati verso l'esterno solo per il corretto svolgimento delle attività Aziendali nel rispetto delle regole e delle norme cogenti.
- VII. La conformità con i requisiti legali e con i principi legati alla sicurezza dei dati nei contratti con le terze parti.
- VIII. Il rispetto delle disposizioni di legge, di statuti, regolamenti e obblighi contrattuali, nonché di ogni requisito inerente la sicurezza dei dati.
- IX. Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi.
- X. Ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione, prevenire l'accesso non autorizzato alle sedi e ai singoli locali Aziendali dove sono gestiti i dati e deve essere garantita la sicurezza delle apparecchiature.
- XI. Le autorizzazioni di accesso ai dati devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere ai soli dati di cui necessita, e devono essere periodicamente sottoposte a revisione.
- XII. Che sia gestito in modo tempestivo ogni incidente, ovvero tutti devono notificare qualsiasi problema relativo alla sicurezza.

La Direzione