Politica per la Sicurezza delle Informazioni

1. Scopo

La presente politica definisce il quadro generale per la gestione della sicurezza delle informazioni all'interno di A-thon Srl.

L'obiettivo primario è garantire la riservatezza, l'integrità e la disponibilità delle informazioni, proteggendole da accessi non autorizzati, divulgazione, uso improprio, alterazione, distruzione o perdita.

2. Ambito di applicazione

Questa politica si applica a tutti i dipendenti, collaboratori, fornitori e terze parti che hanno accesso alle informazioni dell'organizzazione, indipendentemente dal formato (digitale, cartaceo o altro).

3. Principi fondamentali

- **Responsabilità:** Tutti i membri dell'organizzazione sono responsabili della protezione delle informazioni.
- **Confidenzialità:** Le informazioni devono essere protette da accessi non autorizzati.
- **Integrità:** Le informazioni devono essere accurate e complete, e protette da modifiche non autorizzate.
- **Disponibilità:** Le informazioni e i sistemi informativi devono essere accessibili e utilizzabili quando necessari.

4. Obiettivi

- Implementare e mantenere un sistema di gestione della sicurezza delle informazioni (SGSI) conforme agli standard internazionali.
- Identificare, valutare e trattare i rischi per la sicurezza delle informazioni.
- Proteggere le informazioni da accessi non autorizzati, divulgazione, uso improprio, alterazione, distruzione o perdita.
- Garantire la conformità alle leggi, ai regolamenti e ai contratti applicabili.
- Sensibilizzare tutti i dipendenti sulla sicurezza delle informazioni.

5. Responsabilità

- **Direzione:** ha la responsabilità generale di implementare e mantenere la presente politica.
- **Tutti i dipendenti:** sono responsabili di seguire le procedure di sicurezza e di segnalare eventuali incidenti di sicurezza.

6. Misure di sicurezza

Le misure di sicurezza includono, ma non si limitano a:

- **Controllo degli accessi:** utilizzo di autenticazione forte, autorizzazioni basate sui ruoli e monitoraggio delle attività.
- **Protezione fisica adeguata delle sedi aziendali:** è necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature**.**
- **Protezione dei dispositivi:** utilizzo di antivirus, firewall, crittografia ove ritenuto necessario a salvaguardia delle informazioni.
- **Gestione delle password:** imposizione di password complesse e uniche, e cambio periodico.
- **Sensibilizzazione:** organizzazione di corsi di formazione sulla sicurezza informatica per tutti i dipendenti.
- **Gestione degli incidenti:** Definizione di procedure per la gestione degli incidenti di sicurezza.
- **Sicurezza informatica by design:** gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- **Continuità operativa:** Pianificazione e test di piani di ripristino in caso di disastro.

7. Revisione

La presente politica sarà rivista periodicamente per assicurarne l'adeguatezza e l'efficacia.

Stato	Redatto da	Approvato da	Livello confidenzialità	Lista di distribuzione
Approvato	Marta De Munari	Marco Solfa	Pubblico	—