Politica per la Sicurezza delle Informazioni

Per il Centro Formazione Professionale Mary Boyd Sas la gestione della sicurezza delle informazioni ha come obiettivo primario preservare la riservatezza, l'integrità e la disponibilità delle informazioni, al fine di salvaguardare il patrimonio rappresentato dagli asset e dalle conoscenze aziendali, soddisfare i requisiti delle parti interessate e tutelare le persone fisiche di cui si trattano i dati personali.

Per le caratteristiche dei servizi che la società offre ai propri clienti e per il valore che rappresentano le informazioni nel proprio business, la politica per la sicurezza delle informazioni rappresenta un indirizzo strategico fondamentale e prioritario.

La politica per la sicurezza delle informazioni per la società è costituita da un insieme di attività che comprendono: l'identificazione degli asset primari, la gestione dei rischi, dei sistemi e della rete, l'identificazione delle vulnerabilità e degli incidenti, il controllo degli accessi, la gestione della privacy e della compliance, la valutazione dei danni e tutti gli altri aspetti che possono impattare sulla gestione della sicurezza delle informazioni.

La società impegna, quindi, la propria organizzazione a sviluppare e manutenere un sistema di gestione della sicurezza delle informazioni nell'ambito delle attività svolte e dei servizi erogati al fine di garantire la disponibilità l'integrità e la riservatezza dei dati.

La presente politica si applica a tutto il personale interno e quello delle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione ed erogazione di servizi formativi. La sede di riferimento è sita in Salerno - alla Via Posidonia n. 55.

Tutte le persone che lavorano e/o collaborano con la società sono impegnate a rispettare i seguenti principi:

1. **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate;
2. **Integrità**: salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;
3. **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
4. **Controllo**: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità**: garantire una provenienza affidabile dell'informazione;
6. **Privacy**: garantire la protezione ed il controllo dei dati personali.

La Direzione è fortemente impegnata a una grande responsabilizzazione di tutte le persone che lavorano per e con la società nel garantire la rigorosità del proprio operato per adempiere, con la massima attenzione, ai compiti assegnati.

In particolare, questo obiettivo è perseguito attraverso l'impegno a garantire:

- il rispetto delle leggi e normative vigenti;
- l'efficienza operativa e affidabilità dei processi di sviluppo prodotti e servizi correlati;
- le condizioni di salute e sicurezza sui luoghi di lavoro per il personale e per i collaboratori;
- la continuità e l'efficienza dei processi organizzativi e operativi al fine di prevenire e ridurre al minimo l'impatto degli incidenti volontari o casuali sulla sicurezza dei dati/informazioni gestite;
- la protezione dei mezzi resi disponibili, ed il loro corretto utilizzo;

- la riservatezza, la correttezza e la disponibilità delle informazioni gestite e la salvaguardia della proprietà intellettuale;
- l'adozione di misure di prevenzione di anomalie di processo/prodotto/servizio.

Per dare attuazione alla propria politica della sicurezza delle informazioni, la Direzione ha sviluppato e si impegna a mantenere un sistema di gestione sicura delle informazioni conforme ai requisiti specificati della Norma ISO/IEC 27001.

La Direzione con la presente politica si impegna a garantire che:

1. l'organizzazione abbia piena conoscenza delle informazioni gestite e valuti di volta in volta la loro criticità, al fine di agevolare l'implementazione di adeguati livelli di protezione;
2. l'accesso alle informazioni avvenga in modo sicuro e adatto a prevenire i trattamenti non autorizzati o realizzati senza i diritti necessari;
3. l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
4. l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, siano adeguatamente formate e abbiano piena consapevolezza delle problematiche relative alla sicurezza;
5. le anomalie e gli incidenti aventi ripercussioni sul sistema informativo, sui servizi 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;
6. l'accesso alla sede ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
7. siano assicurati la conformità ai requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
8. la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi siano gestiti al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni;
9. la business continuity aziendale e il disaster recovery siano attuati attraverso l'applicazione di procedure di sicurezza stabilite;
10. i trattamenti dei dati personali, sia nei casi in cui la società operi in qualità di Titolare che nei casi in cui operi per conto terzi in qualità di Responsabile del Trattamento, avvengano nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali GDPR 679/2016.

La Direzione d si impegna infine a:

- adottare un sistema di gestione sicura delle informazioni conforme ai requisiti specificati della norma ISO/IEC 27001;
- mantenere costantemente monitorato il grado di conformità del sistema alle norme e leggi applicabili di natura cogente e volontaria, e gli obblighi contrattuali pertinenti l'ambito di applicazione del SGSI;
- garantire mezzi e risorse idonee al suo mantenimento e miglioramento continuo, in particolare per quanto attiene la mitigazione/riduzione dei livelli di rischio sulla sicurezza delle informazioni e l'adozione di misure idonee a prevenire situazioni anomale e di emergenza;
- rendere consapevoli tutte le persone dell'organizzazione degli obblighi e delle responsabilità di ciascuno nella gestione della sicurezza delle informazioni e delle conseguenze in caso di eventi, dolosi e colposi, relativi all'utilizzazione non autorizzata, modifica o distruzione di informazioni critiche.

La politica della sicurezza delle informazioni viene costantemente aggiornata e verificata, attraverso un riesame annuale, per assicurare la coerenza con le finalità strategiche dell'organizzazione. La politica è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso la sua pubblicazione sul sito.

Salerno, 01.06.2022

La Direzione