POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

Mustard è una un'agenzia indipendente di comunicazione creativa digitale nata per supportare le aziende clienti nei progetti di potenziamento delle loro relazioni con i propri consumatori, e opera nei seguenti ambiti:

- ideazione, realizzazione e commercializzazione di concorsi online
- ideazione, realizzazione e commercializzazione di siti web e di e-commerce
- ideazione, realizzazione e commercializzazione di applicazioni mobile
- strategia di sviluppo del brand
- advertising (spot, out of home, campagne digital, branded content, materiali GDO)
- social media

La presente Politica della Sicurezza delle Informazioni rappresenta un indirizzo strategico fondamentale e prioritario, in considerazione delle caratteristiche dei servizi che Mustard offre ai propri clienti e per il valore che rappresentano le informazioni nel proprio business.

Mustard, con l'obiettivo di garantire la sicurezza delle informazioni e conformemente ai requisiti specificati della norma ISO/IEC 27001:2022 e alle leggi vigenti, ha implementato e si impegna a mantenere un sistema di gestione sicura delle informazioni nell'ambito delle proprie attività.

La Gestione della Sicurezza delle Informazioni si concentra sulla protezione dei dati, preservando il patrimonio costituito dalle conoscenze aziendali e dai dati personali dei clienti. La Politica della Sicurezza delle Informazioni definisce e organizza la riservatezza, l'integrità e la disponibilità delle informazioni, gestendo aspetti tecnici, di management e di business.

Mustard adotta un approccio "by design" prestando particolare attenzione alla progettazione, gestione e manutenzione della propria infrastruttura tecnologica, fisica ed organizzativa.

La politica per la sicurezza delle informazioni di Mustard si applica a tutto il personale interno e quello delle terze parti che collaborano alla gestione delle informazioni nella progettazione, realizzazione ed erogazione dei servizi.

Tutte le persone che lavorano e/o collaborano con Mustard si impegnano a rispettare i seguenti principi:

1) **Riservatezza**: garantire 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**: preservare la consistenza delle informazioni da modifiche non autorizzate e garantire che le informazioni non subiscano 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 strumenti associati quando ne fanno richiesta, garantendo accesso, usabilità e confidenzialità dei dati e riducendo i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, ecc.);

4) **Controllo**: gestire i dati attraverso processi e strumenti sicuri e testati;

5) **Autenticità**: garantire una provenienza affidabile dell'informazione;

6) **Privacy**: proteggere e controllare i dati personali.

Mustard garantisce nell'erogare i propri servizi:

- osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione del SGSI (sistema di gestione della sicurezza delle informazioni)
- rispetto delle normative vigenti e degli standard internazionali di sicurezza per la propria infrastruttura tecnologica e organizzativa
- selezione di partner affidabili dal punto di vista della gestione in sicurezza delle informazioni e della protezione dei dati personali.

La presente politica della sicurezza delle informazioni garantisce che:

1) l'organizzazione abbia piena conoscenza delle informazioni gestite e valuti la loro criticità, per adottare 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 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) la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;

8) la business continuity aziendale e il disaster recovery, siano garantite attraverso l'applicazione di procedure di sicurezza stabilite;

9) il trattamento dei dati personali avvenga nel rispetto del Regolamento (UE) 2016/679.

10) siano garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

11) siano eseguiti penetration test periodici nelle infrastrutture e negli applicativi per valutare la resilienza dei sistemi ad attacchi esterni ed evincere eventuali vulnerabilità e consentirne la successiva attenuazione.

POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

La Direzione è fortemente impegnata a responsabilizzare tutte le persone coinvolte nelle attività di Mustard, garantendo la rigorosità del proprio operato. Questo impegno si traduce:

- nel rispetto delle leggi e normative vigenti;
- nell'efficienza operativa e affidabilità dei processi di sviluppo prodotti e servizi correlati;
- nelle condizioni di salute e sicurezza sui luoghi di lavoro per il personale e terzi;
- nella continuità ed 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;
- nella protezione dei mezzi resi disponibili e nel loro corretto utilizzo;
- nella riservatezza, correttezza e disponibilità dei dati/informazioni e nella salvaguardia della proprietà intellettuale;
- nell'adozione di misure di prevenzione di anomalie di processo/prodotto/servizio.

La politica della sicurezza delle informazioni viene costantemente aggiornata e verificata, attraverso riesami periodici, per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso la sua pubblicazione sul sito.

Milano, 15 Febbraio 2024

LA DIREZIONE