Politica sulla Sicurezza Informatica

Il nostro approccio alla sicurezza della tecnologia dell'informazione (IT)

Il Gruppo F.I.L.A. è tra i principali operatori a livello mondiale specializzato nella ricerca, nel design, nella produzione e nella vendita di strumenti di espressione creativa. Il Gruppo progetta, produce e confeziona strumenti e supporti per disegnare, colorare, pitturare e modellare, per i bambini, i giovani e gli adulti. A oggi conta su un'offerta di oltre 25 brand iconici e migliaia di prodotti disponibili in tutti i continenti.

Teniamo sempre un comportamento responsabile nei confronti di tutti i nostri stakeholder nella gestione della società, combinando il rispetto delle persone, dell'ambiente naturale e delle comunità, e la sostenibilità fa quindi parte delle nostre Finalità, Visione, Missione e Valori delineati nel nostro Codice etico e nelle operazioni quotidiane.

Questa politica, insieme al nostro Codice Etico e al Modello di Corporate Governance, deve essere adottata da tutte le consociate e fa parte del Modello di Organizzazione, Gestione e Controllo del Gruppo, in conformità ai principi e agli obiettivi del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001.

Il Gruppo protegge il suo patrimonio aziendale al massimo livello delle sue capacità tecniche e delle risorse disponibili, suddivise nei seguenti elementi fondamentali: persone, beni (asset) e informazioni. La condizione necessaria per lo svolgimento di tutte le attività del Gruppo F.I.L.A. è la protezione dell'informazione gestita per mezzo di criteri, misure e controlli di sicurezza proporzionali ai rischi e al valore dell'informazione stessa.

La sicurezza informatica del Gruppo F.I.L.A. è un requisito fondamentale per garantire l'affidabilità delle informazioni trattate, nonché l'efficacia e l'efficienza dei servizi forniti dal Gruppo. La Sicurezza Informatica ha come obiettivo primario la protezione delle informazioni, dei dati personali e della conservazione digitale e degli elementi attraverso i quali i dati vengono gestiti proteggendoli dalle minacce, siano esse organizzative o tecnologiche, interne o esterne, accidentali o intenzionali, garantendo la loro riservatezza, integrità e disponibilità e il rispetto della legislazione vigente applicabile.

La sicurezza informatica è un aspetto fondamentale della nostra attività, in quanto ci consente di proteggere i nostri "asset", come un sito, un computer o un'automobile, contro le minacce informatiche, e allo stesso tempo minimizzare l'impatto in caso di vulnerabilità dovuta al superamento delle difese implementate.

Nel Gruppo F.I.L.A., gli obiettivi di sicurezza informatica possono essere riassunti come segue:

- Riservatezza, cioè garantire la prevenzione di accessi abusivi o non autorizzati a informazioni, servizi e sistemi
- Integrità, vale a dire assicurare che le informazioni non siano state alterate da incidenti o abusi
- **Sicurezza**, le informazioni devono essere mantenute e protette da ogni possibile minaccia esterna, sia fisica sia logica.
- Disponibilità, o la garanzia dell'accesso ai servizi di informazione e di rete da parte del personale incaricato in relazione alle esigenze di lavoro
- Coerenza, cioè controllare che siano disponibili strumenti che ci permettono di comprendere se ciò che ci aspettiamo accade realmente
- Controllo, cioè avere la possibilità di regolare l'accesso al sistema di dati e di limitare l'accesso e suddividere gli utenti per gruppi, funzionalità, ecc.
- Supervisione delle operazioni che vengono eseguite, cioè controlli o audit.

La mancanza di un adeguato livello di sicurezza dei dati, in termini di riservatezza, disponibilità ed integrità, può avere come conseguenze la perdita di vantaggio competitivo, di immagine, di clienti, di fatturato ed una conseguente significativa perdita finanziaria. A tutto questo bisogna, inoltre, aggiungere il rischio di incorrere in sanzioni legate a violazioni delle normative vigenti.

Pertanto la sicurezza del sistema informativo viene ottenuta implementando una serie di misure di sicurezza adeguate, ovvero procedure, meccanismi tecnici o pratiche che riducano i rischi cui risulta esposto il patrimonio informativo nel suo complesso.

Orientiamo le nostre attività al rispetto della legislazione vigente, con particolare riferimento ai Codici applicabili in materia di protezione dei dati personali in tutti i paesi in cui operiamo, non solo al fine di evitare il rischio di un coinvolgimento aziendale, ma soprattutto per garantire un adeguato livello di sicurezza dei dati personali del Gruppo e del suo sistema informativo.

Ci impegniamo a mantenere i più alti standard etici possibili e a rispettare tutte le leggi applicabili in tutti i paesi in cui operiamo commercialmente. Crediamo fermamente di avere la responsabilità di operare nel rispetto delle norme dei paesi in cui siamo presenti, distinguendoci come un'impresa capace di esportare i Valori che permeano le nostre azioni, promuovendoli nelle comunità in cui operiamo.

Ambito di questa politica

Questa politica si applica a F.I.L.A. S.p.A., alle sue controllate, alle entità in cui detiene una partecipazione di maggioranza e alle strutture che gestisce. Ci impegniamo a lavorare con i nostri partner commerciali e a incoraggiarli a sostenere i principi di questa politica e ad adottare politiche simili all'interno delle loro attività.

A livello locale, ogni azienda deve adottare regole e procedure più rigorose, come necessario e in conformità con le leggi e i regolamenti locali. Nello svolgimento delle attività di gestione, coordinamento e supervisione, F.I.L.A. S.p.A. rispetta l'autonomia gestionale di ciascuna affiliata del proprio Gruppo, gestendo e controllando il business complessivo, secondo gli interessi legittimi degli azionisti di maggioranza e di minoranza, tenendo conto delle esigenze di riservatezza e delle leggi locali applicabili.

Crediamo fermamente di avere la responsabilità di operare nel rispetto delle norme dei paesi in cui siamo presenti, distinguendoci come un'impresa capace di esportare i Valori che permeano le nostre azioni, promuovendoli nelle comunità in cui operiamo. La finalità di questa politica è offrire una guida agli amministratori, ai funzionari, ai dipendenti, agli agenti, ai consulenti, agli intermediari, alle joint venture controllate e ad altri rappresentanti di terze parti di F.I.L.A. per garantire il rispetto della normativa applicabile e dei nostri valori e politiche.

Il Gruppo F.I.L.A. si impegna a un miglioramento continuo delle sue politiche e dei suoi programmi, facilitando l'adozione a livello locale di tutte le procedure, regole e istruzioni necessarie affinché i principi stabiliti in questa Politica siano applicabili e monitorati, al fine di ottenere un impatto positivo. Adottando questa politica, riteniamo di contribuire a una migliore condizione delle generazioni presenti e future, fornendo strumenti per una migliore qualità di vita.

Principi generali

Nelle nostre strategie e operazioni, teniamo in considerazione i seguenti principi riguardo la sicurezza IT:

- **Sistemi informativi aziendali**: i dipendenti e i collaboratori interni dispongono di tutti gli strumenti necessari per svolgere i compiti assegnati. Gli strumenti e le applicazioni software forniti sono strumenti di lavoro e devono essere utilizzati per questi scopi: i dati presenti all'interno degli strumenti di lavoro (compresi i sistemi di posta elettronica e i sistemi di file locali/di rete, nonché le posizioni di archiviazione dei dati nel Cloud) sono considerati dati aziendali e come tali di proprietà della Società. Di conseguenza, l'azienda può avere accesso completo a questi dati e gli utenti non potranno avere aspettative di privacy rispetto alle informazioni inviate, ricevute o memorizzate. Usi impropri dei sistemi aziendali comprendono l'elaborazione, la trasmissione, il recupero, l'accesso, la visualizzazione, la memorizzazione, la stampa e in generale la diffusione di materiali e dati fraudolenti, molesti, minacciosi, illegali, razzisti, di orientamento sessuale, osceno, intimidatorio, diffamatorio o comunque non congruente con il comportamento professionale. Pertanto, nessun dato di questo tipo deve essere presente nella rete di F.I.L.A., sui Personal Computer, nelle applicazioni (come e-mail, portali Intranet, ecc.). Inoltre, gli utenti dei sistemi aziendali non devono utilizzare le infrastrutture per condurre attività commerciali personali, vendere prodotti, o per qualsiasi altra attività commerciale diversa da quelle espressamente previste dalla direzione aziendale
- **Accesso alle informazioni:** L'accesso alle informazioni da parte di ogni utente deve essere limitato solo alle informazioni di cui ha bisogno per l'esecuzione dei suoi compiti (principio del "bisogno di sapere"). La divulgazione e la trasmissione di informazioni all'interno, così come all'esterno, devono essere basate sullo stesso principio. Il Gruppo F.I.L.A. applicherà questa politica impostando profili e diritti utente adeguati, per limitare la possibilità di accedere alle informazioni in conformità con il principio di cui sopra. Condividere le informazioni di accesso dell'utente, come account e password, con altri dipendenti o individui, non memorizzandole in modo adeguato e sicuro o non aggiornando le informazioni di accesso regolarmente e secondo le Linee guida operative di sicurezza informatica, è considerato un uso improprio dei sistemi e delle informazioni aziendali e, come tali, sanzionate.
- Personale e sicurezza: Il Gruppo F.I.L.A. pianifica e realizza attività di training e informazione rivolte al personale, con particolare attenzione alla sicurezza informatica e al corretto utilizzo delle apparecchiature aziendali. Il personale deve essere tenuto a garantire un livello minimo di sicurezza per le apparecchiature assegnate. Il furto, il danneggiamento o la perdita di strumenti di lavoro devono essere prontamente segnalati. Il personale (compresi i consulenti e i collaboratori esterni) deve sottoscrivere clausole di riservatezza.

- **Incidenti informatici e anomalie**: Tutti i dipendenti sono tenuti a rilevare e notificare a chi di dovere qualsiasi problema relativo alla sicurezza del Gruppo e della Società. Tutti i dipendenti sono tenuti a portare avanti le attività di lavoro quotidiane e a utilizzare i sistemi aziendali (con particolare riferimento, ma senza alcuna limitazione, agli strumenti di collaborazione come E-Mail, Microsoft Teams, Microsoft Sharepoint) con la dovuta cura e attenzione nei confronti di messaggi sospetti, allegati e richieste di contatto.
- **Sicurezza fisica**: L'accesso agli edifici e ai locali rilevanti per la protezione degli asset può avvenire solo dopo l'identificazione delle parti autorizzate. L'identificazione e la progettazione di contromisure di sicurezza fisica devono considerare sia la possibilità di minacce fisiche sia la legislazione applicabile. La manutenzione dell'attrezzatura deve essere eseguita secondo le istruzioni del produttore o con procedure documentate per garantire la disponibilità e l'integrità del servizio
- **Sicurezza IT**: Nell'identificazione e progettazione di contromisure di sicurezza informatica è necessario considerare sia la possibilità di tentativi di accesso non autorizzati interni ed esterni sia la legislazione applicabile e qualsiasi altro vincolo rilevante. Gli utenti non devono sfruttare nessuna vulnerabilità o deficienza del sistema di sicurezza informatica per danneggiare i sistemi o i dati, ottenere risorse per le quali non sono autorizzati, appropriarsi illegalmente delle risorse di altri utenti o ottenere accesso a sistemi per i quali non hanno le autorizzazioni necessarie. Al contrario, gli utenti devono avere cura di comunicare all'amministratore del sistema, per iscritto, qualsiasi malfunzionamento del sistema che possa suggerire la possibile perdita di stabilità o affidabilità dello stesso
- **Controlli**: I sistemi d'informazione devono essere controllati periodicamente così come l'applicazione delle procedure operative. Il personale della divisione IT è autorizzato a effettuare interventi nel sistema informatico del Gruppo finalizzati a garantire la sicurezza e la protezione del sistema stesso, nonché per ulteriori motivi tecnici e/o di manutenzione (es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware ecc.)

I controlli di sicurezza attuati al fine di proteggere le risorse informatiche aziendali sono implementati attraverso:

- l'attuazione e la conformità alle politiche in tutte le aree organizzative, procedurali e tecnologiche in modo coerente rispetto agli obiettivi definiti
- l'adeguata assegnazione di compiti e responsabilità all'interno del Gruppo per l'attuazione delle politiche
- la verifica (nell'ambito dell'analisi dei rischi informatici) del livello di efficacia delle misure implementate, ricorrendo anche a valutazioni periodiche delle vulnerabilità eseguite da soggetti esterni e indipendenti.

Il mancato rispetto delle disposizioni di questa politica di sicurezza informatica sarà soggetto a sanzioni disciplinari, come appropriato.

La dirigenza senior di F.I.L.A. svolge un ruolo strategico nella piena attuazione di questa Politica assicurando il coinvolgimento di tutto il personale e di coloro che collaborano con F.I.L.A. e la coerenza dei loro comportamenti con i valori incarnati da questa Politica.

Questa Politica viene comunicata all'interno dell'organizzazione e viene resa disponibile online per tutte le parti interessate sul sito web www.filagroup.it.

F.I.L.A. incoraggia chiunque venga a conoscenza di fatti o comportamenti contrari al Codice Etico, alle politiche e alle norme interne, alle leggi o ai regolamenti della Società, a fare una segnalazione nella massima riservatezza. Assicurando la riservatezza dell'identità dell'informatore, F.I.L.A. offre i seguenti canali per inoltrare la segnalazione:

- E-mail: whistleblowing.fila@gmail.com
- Inviare un'e-mail a: odv@fila.it Organismo di Vigilanza, F.I.L.A. Fabbrica Italiana Lapis ed Affini S.p.A. Via XXV Aprile, 5 20016 Pero (MI).

Ottobre 2021

CEO DEL GRUPPO – MASSIMO CANDELA