INEVO
INSPIRING EVOLUTION

Via Piave 4, 31020
San Polo di Piave (TV)
Italy

Ph. +39 0422 1345 111
info@inevo.eu

POLITICA DI SICUREZZA DELLE INFORMAZIONI INEVO

SCOPO

La politica di Sicurezza delle Informazioni di Inevo ha come scopo principale proteggere la riservatezza, l'integrità e la disponibilità delle informazioni aziendali, prevenendo minacce interne ed esterne. La politica definisce le modalità con cui le informazioni vengono trattate all'interno dell'organizzazione, prevenendo accessi non autorizzati, divulgazione non prevista, alterazioni o distruzione dei dati. Essa stabilisce anche le modalità di risposta agli incidenti di sicurezza e favorisce la conformità alle normative e alle migliori pratiche di sicurezza informatica.

CAMPO DI APPLICAZIONE

La presente politica si estende a tutte le attività, risorse e informazioni relative alla progettazione, sviluppo, realizzazione e assistenza di stampi per materiali plastici e allo stampaggio a iniezione di materie plastiche, gestite all'interno della sede aziendale. La politica si applica a tutte le informazioni aziendali, inclusi i dati tecnici, progettuali, operativi e di assistenza, nonché a tutti i sistemi informatici, infrastrutture, dispositivi e reti utilizzati per la gestione e il trattamento di tali informazioni. Essa coinvolge tutto il personale interno e le terze parti eventualmente coinvolte, come fornitori o consulenti, che trattano informazioni sensibili legate alle attività aziendali. La gestione e la diffusione delle informazioni esterne all'azienda sono consentite solo per il corretto svolgimento delle operazioni aziendali, sempre nel rispetto delle normative di sicurezza e privacy applicabili.

NORMATIVE DI RIFERIMENTO

La politica di **S**icurezza delle **I**nformazioni di INEVO è stata definita in conformità agli standard internazionali, come la ISO/IEC 27001, e alle normative relative alle migliori pratiche nella gestione della sicurezza delle informazioni. Questa politica è stata sviluppata tenendo conto dei rischi specifici che caratterizzano l'azienda e dei relativi requisiti di business, al fine di garantire che la protezione delle informazioni e la gestione dei rischi siano pienamente allineate alle esigenze aziendali e conformi agli obblighi normativi.

PRINCIPI FONDAMENTALI DELLA POLITICA

La politica di sicurezza di Inevo rappresenta l'impegno dell'organizzazione nei confronti di clienti, partner e terze parti per garantire la protezione delle informazioni, dei sistemi fisici, logici e organizzativi utilizzati nel loro trattamento. In questo contesto, l'azienda si guida dai seguenti principi fondamentali:

Gestione e Protezione delle Informazioni

- Identificare e valutare la criticità delle informazioni trattate per garantire adeguati livelli di protezione.

Via Piave 4, 31020
San Polo di Piave (TV)
Italy

Ph. +39 0422 1345 111
info@inevo.eu

- Assicurare l'accesso sicuro ai dati, prevenendo trattamenti non autorizzati o privi delle necessarie autorizzazioni.
- Adottare procedure di sicurezza adeguate in collaborazione con terze parti, assicurandosi che siano consapevoli delle problematiche relative alla sicurezza.
- Stabilire regole chiare per l'uso delle informazioni, dei beni e degli strumenti aziendali.

Risorse e Consapevolezza

- Definire ruoli e responsabilità specifiche per tutto il personale, coinvolgendo anche terze parti con incarichi chiave.
- Destinare risorse adeguate per la sicurezza fisica, logica e organizzativa.
- Promuovere la consapevolezza sui rischi legati alla sicurezza informatica tra dipendenti, collaboratori e terze parti.
- Garantire che tutto il personale, indipendentemente dal livello gerarchico, comprenda l'importanza della protezione delle informazioni.

Sicurezza Fisica e Logica

- Limitare l'accesso agli uffici e alle aree sensibili esclusivamente al personale autorizzato.
- Proteggere i sistemi informativi aziendali da accessi non autorizzati e minacce esterne.
- Assicurare l'accesso protetto alle informazioni, prevenendo trattamenti non autorizzati o privi delle necessarie autorizzazioni.

Prevenzione e Gestione degli Incidenti

- Predisporre misure di prevenzione, reazione e gestione degli incidenti di sicurezza per minimizzare impatti operativi.
- Riconoscere e gestire tempestivamente anomalie e incidenti che potrebbero influire sul sistema informativo, sui servizi o sulla sicurezza aziendale, utilizzando sistemi efficienti di comunicazione e reazione.
- Definire processi chiari per garantire la continuità operativa (business continuity) e il recupero in caso di disastri (disaster recovery) durante eventi critici.

Gestione dei Dati

- Stabilire misure specifiche per proteggere i dati sensibili e garantire la conformità alle leggi sulla privacy, come il GDPR.
- Definire procedure per la creazione di copie di backup regolari e per la gestione del recupero dei dati in caso di incidente.
- Mantenere la conformità con le normative vigenti, le disposizioni contrattuali e regolamentari, in particolare in materia di protezione dei dati.
- Assicurare che le informazioni personali di terzi siano trattate secondo i principi di liceità, proporzionalità e pertinenza.

INEVO
INSPIRING EVOLUTION

Via Piave 4, 31020
San Polo di Piave (TV)
Italy

Ph. +39 0422 1345 111
info@inevo.eu

Compliance e Miglioramento Continuo

- Rispettare le normative locali e internazionali relative alla sicurezza delle informazioni.
- Stabilire un processo di revisione periodica della politica di sicurezza per adattarla alle nuove minacce o cambiamenti aziendali.
- Adottare un processo di miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni, pianificando, verificando e aggiornando le misure per proteggere il patrimonio informativo aziendale.

La politica di Sicurezza delle Informazioni è resa accessibile a tutto il personale, ai collaboratori, ai clienti e ai fornitori attraverso il sito internet aziendale, dove è disponibile la versione più aggiornata.

La direzione è incaricata della gestione sicura delle informazioni, adattandosi ai cambiamenti del contesto aziendale e di mercato. Questa responsabilità include la valutazione di possibili azioni da intraprendere in risposta a eventi quali: significativi sviluppi del business, nuove minacce rispetto a quelle considerate nelle attività di analisi dei rischi, gravi incidenti di sicurezza, e modifiche nelle normative o leggi relative alla protezione sicura delle informazioni.

DATA

14/11/2024

La Direzione Generale