



## **POLITICA DI GESTIONE DELLE INFORMAZIONI**

### **Tratto dal modello di gestione delle informazioni**

#### LA POLITICA SULLA SICUREZZA DELLE INFORMAZIONI

L'azienda considera la Sicurezza delle Informazioni un aspetto primario della propria organizzazione e interesse di ogni utente.

La reputazione dell'azienda si basa sulla corretta gestione degli asset fisici, informativi e del personale: per preservarla è quindi fondamentale un modello della sicurezza che miri a proteggere i processi e le informazioni da un'ampia gamma di minacce e a minimizzarne l'impatto sulla continuità operativa e sui possibili disagi per gli utenti.

La posizione dell'azienda sulla Sicurezza inoltre contribuisce ad obiettivi di sicurezza più ampi, incluso il miglioramento della resilienza informatica dell'intero eco-sistema imprenditoriale, rispondendo alle aspettative delle Pubbliche Autorità, degli Enti Pubblici, degli Enti di controllo e dei Clienti, dei Dipendenti e degli Utenti.

La Direzione promuove una efficace Governance dell'Information Security nel modo seguente:

- Istituyendo una cultura della sicurezza delle informazioni che promuove un programma efficace di sicurezza delle informazioni e il ruolo di tutto il personale nel proteggere le informazioni, i sistemi e le infrastrutture aziendali.
- Definendo e comunicando in modo chiaro ruoli e responsabilità in ambito di gestione della sicurezza delle informazioni in tutta l'organizzazione comunale;
- Fornendo risorse adeguate per supportare efficacemente il programma di sicurezza (Information Security);
- Scegliendo la ISO/IEC 27001 come standard di riferimento per il proprio Sistema di Gestione della Sicurezza delle Informazioni.

La politica e le procedure correlate che forniscono informazioni dettagliate sulle istruzioni da seguire, si applicano a tutte le funzioni, dipendenti e terze parti dell'azienda che utilizzano strutture ICT, attrezzature e sistemi aziendali, o hanno accesso o la custodia di informazioni aziendali.

La Politica sulla Sicurezza dell'Informazione è rivista regolarmente o in caso di cambiamenti significativi, con l'obiettivo di assicurare la sua continua idoneità, adeguatezza ed efficacia.

#### Obiettivi

I principali obiettivi del Sistema di Gestione della Sicurezza dell'Informazione dell'azienda sono:

- Garantire una protezione dell'informazione adeguata in termini di confidenzialità, integrità e disponibilità;
- Proteggere l'interesse degli Utenti, dei dipendenti e delle terze parti;
- Assicurare la conformità alle leggi e ai regolamenti applicabili in materia di trattamento e protezione dell'informazione;
- Assicurare un modello strutturale alla protezione dell'informazione e alla gestione dei rischi correlati;
- Rispondere in modo efficace alle crescenti minacce ai sistemi informativi e telematici.

Questi obiettivi costituiscono il fondamento per la creazione, l'implementazione, il funzionamento, il monitoraggio, la revisione, la manutenzione e il miglioramento continuo di un efficace sistema di gestione della sicurezza delle informazioni, realizzato in conformità alla norma ISO/IEC 27001.

#### Principi

La progettazione dei processi, il loro continuo miglioramento e, di conseguenza, il trattamento dei dati personali, sono improntati ai sette principi fondamentali:



1. L'approccio aziendale è caratterizzato da misure proattive piuttosto che reattive. Prevede e previene gli eventi invasivi della privacy prima che accadano.
2. L'azienda cerca di ottenere il massimo grado di privacy garantendo che i dati personali siano automaticamente protetti in qualsiasi sistema IT o pratica organizzativa e commerciale.
3. La Privacy è incorporata nella progettazione e nell'architettura dei sistemi IT e dei processi aziendali. Non è aggiunta successivamente come un rimedio, dopo un evento.
4. L'azienda cerca di soddisfare tutti gli interessi legittimi e gli obiettivi in modo da avere una somma positiva "win-win", distaccandosi dalla prospettiva a somma zero, basata su compromessi evitabili.
5. L'azienda garantisce che tutti i dati vengano acquisiti, trattati e conservati in modo sicuro e successivamente distrutti in modo sicuro alla fine del processo. L'organizzazione mira ad un governo sicuro del ciclo di vita delle informazioni dall'inizio alla fine dell'intero processo.
6. Trasparenza e apertura: l'organizzazione dei processi e le tecnologie adottate sono trasparenti e visibili a tutti gli stakeholder ed è verificabile da soggetti indipendenti.
7. Mettere l'utente al centro: consideriamo preminenti gli interessi delle persone, offrendo garanzie come impostazioni predefinite fermamente orientate alla privacy, fornendo complete informazioni e sviluppando in via prioritaria modalità di trattamento rispettose dell'utente.

Pioltello, 20 Maggio 2019

La direzione

Azienda Speciale Servizi

alla Persona e alla Famiglia Futura

AZIENDA SPECIALE SERVIZI  
ALLA PERSONA E ALLE FAMIGLIE "FUTURA"

C.F. 12547300157

IL DIRETTORE