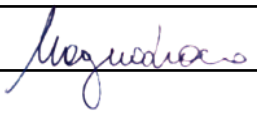
POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

UNI EN ISO 9001:2015 - UNI CEI EN ISO/IEC 27001:2024
INFOSEC_POL
Rev. 2 del 26.11.2024

Data	Versione	Legale Rappresentante	RSGI
10.07.2024	*Rev. 1*		
26.11.2024	**Rev. 2**		

1. Scopo

La presente politica sulla sicurezza delle informazioni ha lo scopo di definire il quadro generale per la protezione delle informazioni aziendali, al fine di garantire la loro confidenzialità, integrità e disponibilità. Questa politica si applica a tutti i dipendenti, collaboratori esterni e chiunque abbia accesso alle risorse informatiche dell'azienda. L'obiettivo primario è di prevenire la perdita, l'uso non autorizzato, la divulgazione, la modifica non autorizzata o la distruzione delle informazioni.

2. Ambito di applicazione

La presente ppoliticaoltica si applica a tutte le informazioni aziendali, indipendentemente dal formato (digitale, cartaceo), compresi:

- Dati personali dei clienti e dei dipendenti
- Proprietà intellettuale (brevetti, marchi, know-how)
- Informazioni finanziarie
- Sistemi informatici (server, workstation, dispositivi mobili, reti)
- Applicazioni software
- Documentazione cartacea e digitale

3. Responsabilità

Responsabile del Sistema Integrato di Gestione (RSIG): Magno Ivano
Responsabile della sicurezza delle informazioni: Magno Ivano
Tutti i dipendenti e collaboratori sono responsabili di:

- Proteggere le informazioni aziendali
- Segnalare eventuali incidenti di sicurezza
- Rispettare le procedure di sicurezza

4. Principi fondamentali

I principi fondamentali della sicurezza delle informazioni sono i seguenti:

- **Confidenzialità**: Proteggere le informazioni da accessi non autorizzati.
- **Integrità**: Garantire l'accuratezza e la completezza delle informazioni.
- **Disponibilità**: Assicurare l'accesso alle informazioni autorizzate quando necessario.
- **Responsabilità**: Definire chiaramente le responsabilità di ciascun individuo coinvolto nella gestione della sicurezza.
- **Trasparenza**: Comunicare chiaramente la politica di sicurezza a tutti i dipendenti.
- **Miglioramento continuo**: Rivedere e aggiornare periodicamente la politica e le procedure di sicurezza.

5. Politiche del sistema

La presente politica sulla sicurezza delle informazioni si integra con le seguenti politiche aziendali, le quali definiscono in modo più dettagliato gli aspetti specifici della gestione della sicurezza:

- **BCK_POL**: Politica per la gestione dei backup.
- **INFOSIS_POL**: Politica per l'uso accettabile dei sistemi informativi.
- **CLASS_POL**: Politica per la classificazione delle informazioni.
- **PASSWORD_POL**: Politica per la gestione delle password.
- **FORMA_POL**: Politica per la sensibilizzazione e formazione.
- **INCIDENT_POL**: Politica per la gestione degli incidenti di sicurezza.
- **ACCESS_POL**: Politica per gli accessi ai sistemi aziendali.
- **EMAIL_POL**: Politica per la gestione delle email
- **PROG_POL**: Politica per l'integrazione della sicurezza dell'informazione nei progetti
- **CRIPT_POL**: Politica per cifratura e mascheramento delle informazioni

6. Procedure del sistema

Le politiche sulla sicurezza delle informazioni sono integrate dalle seguenti procedure specifiche:

- **BCK_PROC**: Procedura per la gestione dei backup
- **CLASS_PROC**: Procedura per la classificazione delle informazioni.
- **PASSWORD_PROC**: Procedura per la gestione delle password.
- **ACCESS_PROC**: Procedura per gli accessi ai sistemi aziendali.
- **DEV_PROC**: Procedura per lo sviluppo web.
- **SERVER_PROC**: Procedura per la gestione server.
- **SMART_PROC**: Procedura per la gestione del telelavoro (smartworking)
- **DEV_PROC**: Procedura per la gestione dello sviluppo web
- **SERVER_PROC**: Procedura di configurazione dei server
- **EMAIL_PROC**: Procedura per la gestione delle email
- **DEL_PROC**: Procedura per la cancellazione sicura delle informazioni
- **CAP_PROC**: Procedura per la gestione e il monitoraggio delle capacità
- **INCIDENT_PROC**: Piano di risposta agli incidenti di sicurezza dell'informazione

7. Altri documenti di riferimento:

Documenti ulteriori che completano e integrano il Sistema sono:

- **Documento di analisi dei rischi e trattamento**: Definisce i rischi identificati per la sicurezza delle informazioni e le misure di mitigazione adottate.
- **Regolamento informatic**o: Definisce le regole generali per l'utilizzo dei sistemi informativi aziendali.
- **Sistema GDPR**: Descrive le modalità di gestione dei dati personali in conformità al Regolamento Generale sulla Protezione dei Dati.

8. Revisione

La politica sarà rivista periodicamente per tener conto dei cambiamenti nell'ambiente di minaccia e delle nuove tecnologie.