Classificazione documento

Pubblico interno	Uso interno	Riservato interno	Segreto interno
☐	✓	☐	☐

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI (ISO/IEC 27001)

1. Obiettivo e Finalità

La presente Policy definisce l'impegno dell'Organizzazione nel proteggere il proprio patrimonio informativo e quello dei propri clienti, partner e fornitori. L'obiettivo principale è garantire la continuità aziendale e minimizzare i danni derivanti da potenziali incidenti di sicurezza, proteggendo le informazioni da ogni tipo di minaccia, interna o esterna, intenzionale o accidentale.

2. I Tre Pilastri della Sicurezza (CIA Triad)

L'Organizzazione si impegna a garantire costantemente tre requisiti fondamentali:

- **Riservatezza**: Le informazioni sono accessibili solo a chi è autorizzato a visionarle.
- **Integrità**: I dati sono protetti da modifiche non autorizzate o accidentali, garantendone l'esattezza.
- **Disponibilità**: Gli utenti autorizzati possono accedere alle informazioni e ai sistemi associati ogni volta che ne hanno necessità.

3. Campo di Applicazione

La presente policy si applica a:

- Tutti i dipendenti, collaboratori, consulenti e fornitori terzi.
- Tutti i dati (digitali, cartacei, verbali) gestiti dall'azienda.
- Tutti i sistemi informatici, reti, dispositivi fisici e servizi cloud aziendali.

4. Principi Chiave e Linee Guida

Gestione degli Accessi (Principio del Minimo Privilegio)

- L'accesso alle informazioni è limitato strictly in base alle necessità lavorative (*Need-to-Know*).
- Ogni utente riceve credenziali univoche e personali.
- È obbligatorio l'uso dell'autenticazione a due fattori (MFA) su tutti i sistemi aziendali.

Sicurezza delle Postazioni di Lavoro (Clean Desk & Clear Screen)

- Gli utenti devono bloccare lo schermo del computer ogni volta che si allontanano dalla postazione.
- Documenti cartacei contenenti dati sensibili non devono essere lasciati incustoditi sulle scrivanie.
- È vietato l'uso di supporti di memoria esterni (USB) non autorizzati dall'ufficio IT.

Protezione da Malware e Gestione delle Vulnerabilità

- Tutti i dispositivi aziendali devono avere sistemi antivirus e software di protezione attivi e aggiornati.

Classificazione documento

Pubblico interno	Uso interno	Riservato interno	Segreto interno
☐	✓	☐	☐

- I sistemi operativi e le applicazioni devono essere patchati tempestivamente secondo i protocolli IT.

Continuità Operativa e Backup

- I dati aziendali critici devono essere sottoposti a backup automatico e periodico.
- I backup devono essere cifrati e testati regolarmente per garantirne il ripristino in caso di incidente.

Consapevolezza e Formazione

- Tutti i dipendenti devono partecipare a sessioni periodiche di formazione sulla sicurezza informatica (es. riconoscimento del phishing).

5. Gestione degli Incidenti

Qualsiasi violazione della sicurezza, reale o sospetta (es. smarrimento di un PC aziendale, email di phishing sospetta, anomalie di sistema), deve essere segnalata immediatamente al Team di Risposta agli Incidenti (CIRT) aziendale secondo la procedura ufficiale.

6. Gestione del Rischio

L'Organizzazione adotta un approccio basato sul rischio. Annualmente viene eseguito un processo di *Risk Assessment* per identificare le minacce, valutare l'impatto di potenziali violazioni e implementare i controlli necessari (selezionati dall'Allegato A della norma ISO 27001).

7. Sanzioni e Violazioni

La conformità alla presente policy è obbligatoria. La mancata osservanza delle regole esporrà il personale a procedimenti disciplinari in conformità con i contratti di lavoro e le normative vigenti.

Modena 02/03/2026

L'Amministratore Unico
Ing. TIMPANI ANDREA VALERIA

PROGETTO PSC Srl
Via del Lavoro, 5 - 41014
Solignano Nuovo (MO)
Tel. 059 797175
P.IVA 03521030365