POLITICA DI CYBERSECURITY AZIENDALE

RECEPIMENTO DELLA DIRETTIVA (UE) 2022/2555 “NIS2” E D.LGS.138/2024

[INTRODUZIONE E NORMATIVA DI RIFERIMENTO]

La sicurezza informatica è una priorità fondamentale per SETTIMA MECCANICA SRL. Questa politica stabilisce l’impegno della Direzione ad adottare un “Modello di Cybersecurity”, finalizzato a proteggere i sistemi informatici aziendali, nonché le informazioni in essi contenute, da minacce interne ed esterne. Nello sviluppo del Modello, SETTIMA identifica la Direttiva UE 2022/2555 “NIS2” quale framework normativo di riferimento, certificandone il pieno recepimento.

[OBIETTIVI]

L’adozione di un’efficace “Modello di Cybersecurity” persegue i seguenti obiettivi:

- proteggere le informazioni aziendali da accessi non autorizzati, modifiche, divulgazioni o distruzioni;
- assicurare la continuità operativa, minimizzando i rischi legati alla Cybersecurity;
- conformarsi alle normative e agli standard di sicurezza informatica applicabili;
- contribuire ad incrementare il livello nazionale e comunitario di cybersecurity, a tutela della società e del mercato.

[AMBITO DI APPLICAZIONE]

Questa politica si applica a tutti i dipendenti, collaboratori, fornitori e terze parti che accedono ai sistemi informatici ed alle informazioni aziendali di SETTIMA.

[PRINCIPI DI CYBERSECURITY]

SETTIMA si impegna ad adottare misure tecniche, operative ed organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete, utilizzati nella propria attività o nella fornitura dei propri servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei propri servizi. Le misure adottate sono basate su un approccio multirischio, mirato a proteggere i sistemi IT e comprendono:

- politiche di analisi e trattamento dei rischi di sicurezza informatica;
- politiche di gestione dei ruoli ed affidabilità, formazione, consapevolezza delle risorse umane;
- politiche di gestione della supply-chain critica IT;
- politiche di gestione degli asset e delle vulnerabilità;
- politiche di continuità operativa, ripristino in caso di disastro e gestione delle crisi;
- politiche di gestione delle identità digitali, dell’autenticazione e dei permessi;
- politiche di sicurezza dei dati, delle piattaforme, delle sedi, delle reti e delle comunicazioni
- politiche di monitoraggio degli eventi di sicurezza e di gestione/notifica degli incidenti.

[RESPONSABILITÀ, FORMAZIONE, CONSAPEVOLEZZA]

- **Direzione aziendale**: esercita il potere decisionale in ambito di Cybersecurity; assegna ruoli e responsabilità; approva le misure di sicurezza; sovrintende alla loro attuazione.
- **Personale IT**: si occupa dell’implementazione, monitoraggio ed aggiornamento delle misure di sicurezza informatiche.
- **Dipendenti**: seguono le politiche, le procedure e le regole di sicurezza; partecipano alla formazione sulla sicurezza; segnalano tempestivamente eventuali incidenti.
- **Fornitori e terze parti**: devono rispettare gli stessi standard di sicurezza applicabili ai dipendenti interni e garantire adeguate misure di protezione.

SETTIMA fornirà regolare formazione ed aggiornamenti sulla sicurezza informatica a tutti i dipendenti, per assicurare la consapevolezza e la comprensione delle migliori pratiche di Cybersecurity. SETTIMA selezionerà fornitori che garantiscano adeguati standard di sicurezza, monitorandone periodicamente il livello di affidabilità.

[REVISIONE DELLA POLITICA]

L’applicazione della presenta politica sarà regolarmente monitorata ed eventualmente integrata, in caso di variazioni significative delle minacce informatiche o nei requisiti normativi. La Direzione di SETTIMA è pertanto impegnata al miglioramento continuo della propria postura di Cybersecurity, per proteggere le proprie risorse, consolidare la fiducia degli stakeholders e contribuire allo sviluppo, alla sicurezza ed al progresso della società.