POLITICA DI CYBERSECURITY AZIENDALE

ATTESTATO DI 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 ONESTIGROUP SPA. 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, ONESTIGROUP si avvale del supporto di una società specializzata in servizi di consulenza in ambito di “Data Governance & Protection”, la quale collabora nella certificazione di quanto attestato nel presente documento. Nello sviluppo del Modello, ONESTIGROUP 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 e alle informazioni aziendali di ONESTIGROUP.

[PRINCIPI DI CYBERSECURITY]

ONESTIGROUP 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 dei rischi e di sicurezza dei sistemi informatici;
- piani di gestione degli incidenti e condivisione delle informazioni sulle minacce;
- piani di continuità operativa.

[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.

ONESTIGROUP fornirà regolare formazione ed aggiornamenti sulla sicurezza informatica a tutti i dipendenti, per assicurare la consapevolezza e la comprensione delle migliori pratiche di Cybersecurity. ONESTIGROUP 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 nelle minacce informatiche o nei requisiti normativi. La Direzione di ONESTIGROUP 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.