Doc:	SGQ-QUA.AL-77-rev.0	*Date:*	17/02/2026	*Page:*	1 / 1

***Subject*: POLITICA ED OBIETTIVI PER LA CYBERSICUREZZA - Direttiva NIS2 (UE 2022/2555)**

Turboden progetta e realizza impianti nel settore delle energie rinnovabili e del recupero di calore. Nell'ambito delle proprie attività, l'azienda tutela la sicurezza delle informazioni proprie e di tutte le parti interessate — garantendone riservatezza, integrità e disponibilità — e assicura la continuità, l'efficacia e l'efficienza dei sistemi di comunicazione (Cybersecurity), per quanto rientri nel proprio controllo diretto. Turboden attua inoltre un monitoraggio costante degli eventi di sicurezza informatica, adottando tempestivamente azioni di ripristino adeguate ed efficaci.

Per perseguire tali obiettivi, Turboden si impegna a:

- **Definire, mantenere, diffondere, migliorare e monitorare un Sistema di Cybersecurity** basato su un processo strutturato di gestione del rischio, volto a garantire la piena conformità ai requisiti della Direttiva (UE) 2022/2555 "NIS2" recepita in Italia con il D.lgs. 138/2024, nonché alle linee guida dell'Agenzia per la Cybersicurezza Nazionale (ACN), attraverso l'implementazione di idonee misure di mitigazione.
- **Assicurare il continuo coinvolgimento del management**, promuovendo la cultura della Cybersecurity a tutti i livelli aziendali, comunicando politica e obiettivi, garantendo le risorse necessarie e responsabilizzando ogni funzione.
- **Nominare, formare e responsabilizzare** le figure previste dalla Direttiva NIS2 per la definizione, applicazione, diffusione e monitoraggio dell'efficacia del Sistema per la Cybersecurity.
- **Favorire la partecipazione attiva e consapevole dei lavoratori**, coinvolgendoli nell'attuazione del Sistema e nel miglioramento continuo.
- **Integrare i requisiti di sostenibilità** nel processo di gestione del rischio Cyber, ove applicabili.

Obiettivi per la Cybersecurity

- **Incrementare il livello complessivo di Cybersecurity**, diffondendo la cultura della sicurezza informatica e garantendo al personale un adeguato livello di competenza.
- **Identificare, valutare, classificare e correggere le vulnerabilità**, assicurando la disponibilità di asset informativi e infrastrutturali adeguati (hardware, software, sistemi di rete) per tutto il personale.
- **Monitorare il Sistema di Cybersecurity** attraverso piani di audit appropriati, che tengano conto dei requisiti normativi e legali applicabili.
- **Preservare la sicurezza dei dati**, garantendone riservatezza, integrità e disponibilità.
- **Tutelare la sicurezza fisica degli asset tangibili e intangibili** garantendo anche l'adeguata manutenzione e provvedendo alla corretta dismissione.
- **Garantire il monitoraggio degli eventi di sicurezza informatica**, fornendo risposte tempestive e adeguate per il ripristino dei dati e delle infrastrutture di comunicazione.
- **Gestire efficacemente le crisi**, mantenendo la continuità operativa e ripristinando la funzionalità degli asset informativi e di comunicazione in caso di disastro.
- **Riesaminare progettazione, pianificazione, realizzazione e manutenzione dei prodotti**, includendo la valutazione dei rischi Cyber secondo quanto previsto dal Sistema di Cybersecurity.
- **Verificare e attuare i requisiti di comunicazione richiesti dalle parti interessate**, assicurando che non siano in conflitto con le misure di mitigazione del rischio adottate.
- **Ridurre l'impatto ambientale dei sistemi di comunicazione**, contribuendo al processo di decarbonizzazione.
- **Assicurare la disponibilità di fornitori, appaltatori e outsourcer conformi ai criteri del Sistema di Gestione per la Cybersecurity**, garantendo comunicazioni sicure con le risorse aziendali.

La presente Politica è comunicata a tutto il personale e resa disponibile tramite i canali aziendali ufficiali.
La Politica è soggetta a riesame annuale, nonché in occasione di evoluzioni del contesto normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.
Ogni aggiornamento è approvato dagli organi di amministrazione e direttivi e comunicato tempestivamente a tutto il personale.

Dr. Paolo Bertuzzi	**Ing. Roberto Bini**	**Ing. Giorgio Fagnani**
Amministratore Delegato, CEO e DdL	*Managing Director*	*Procuratore e QHSE Manager*
(D.Lgs 81/08)		